Windows Server 2016

Krzysztof Wołk

Plik jest zabezpieczony znakiem wodnym

Biblia Windows Server 2016. Podręcznik Administratora

Krzysztof Wołk

Wydawnictwo Psychoskok
Konin 2019

Krzysztof Wołk

„Biblia Windows Server 2016.
Podręcznik Administratora”

Copyright © by **Krzysztof Wołk**, 2019
Copyright © by **Wydawnictwo Psychoskok Sp. z o.o.** 2019

**Wszelkie prawa zastrzeżone. Żadna część niniejszej publikacji nie
może być reprodukowana, powielana i udostępniana w jakiejkolwiek formie bez pisemnej zgody wydawcy.**

Redaktor prowadząca: **Renata Grześkowiak**
Projekt okładki: **Krzysztof Wołk**
Ilustracje na okładce: **Krzysztof Wołk**
Korekta: **Bogusław Jusiak, Joanna Barbara Gębicka**
Skład epub, mobi i pdf: **Kamil Skitek**

http://wolk.pl/

ISBN: **978-83-8119-318-4**

Wydawnictwo Psychoskok Sp. z o.o.
ul. Spółdzielców 3, pok. 325, 62-510 Konin
tel. (63) 242 02 02, kom. 695-943-706

http://www.psychoskok.pl/
http://wydawnictwo.psychoskok.pl/
e-mail:wydawnictwo@psychoskok.pl

Spis treści

Wstęp
O autorze
1. Instalacja
1.1. Wymagania sprzętowe i opis środowiska
1.2. Proces instalacji
2. Post-instalacja
2.1. Czynności post-instalacyjne
2.1.1. Aktualizacje
2.1.2. Zmiana nazwy komputera
2.2. Konfiguracja sieci
2.3. Zarządzanie procesorami i pamięcią operacyjną
3. Active Directory Domain Services
3.1. Czym jest domena?
3.2. Instalacja Active Directory Domain Services
3.3. Wstępna konfiguracja AD DS
3.4. Active Directory Users and Computers
3.5. Active Directory Administrative Center
4. Serwer DNS
4.1. Zapoznanie z konsolą DNS Manager
4.2. Ręczna konfiguracja strefy DNS
4.3. Zarządzanie serwerem DNS
4.4. Zapasowy serwer DNS
5. Serwer DHCP
5.1. Instalacja pierwszego serwera DHCP
5.2. Konfiguracja serwera DHCP
5.3. Zarządzanie serwerem DHCP
5.3.1. DHCP Policies
5.4. Wysoka dostępność DHCP
5.4.1. Konfiguracja klastra DHCP
5.4.2. Split-Scope
6. IIS z FTP oraz Urząd Certyfikacji
6.1. Instalacja roli Web Server (IIS)

6.2. Instalacja Active Directory Certificate Services
6.3. Aktualizacja platformy .NET
6.4. Tworzenie nowych certyfikatów
6.5. Zarządzanie Serwerem IIS
6.6. Uruchamianie Serwera FTP
6.7. IIS i PHP
7. Network Access Protection
7.1. Network Policy and Access Services
7.2. Zarządzanie Network Policy Server
8. VPN, Direct Access i NAT
8.1. Instalacja roli Remote Access
8.2. Konfiguracja VPN i NAT
8.3. Konfiguracja DirectAccess
9. Polisy (Zarządzanie Zasadami Grupy)
9.1. Wybrane nowości w GPO
10. Uprawnienia Sieciowe i na systemie plików
10.1. Uprawnienia sieciowe
10.1.1. Dodatkowe ustawienia udostępnianych plików
10.2. Uprawnienia NTFS
10.3. Autoryzacja metodą CLAIM
10.3.1. Nakładanie uprawnień Claim
10.3.2. Definiowanie Claim Types
10.4. Uprawnienia na systemie plików ReFS
10.5. Zarządzanie drukarkami
10.5.1. Instalowanie drukarek
10.5.2. Zarządzanie dostępem do drukarek sieciowych
11. Serwer Plików
11.1. Instalacja roli Serwera Plików
11.2. Zapoznanie z nowym podejściem do usług plików
11.3. Storage Pools
11.4. Zarządzanie przez Menadżera Serwera Plików
11.4.1. Zarządzanie Osłonami Plików
11.4.2. Zarządzanie Przydziałami
12. Praca zdalna
12.1. Wstępna konfiguracja serwera
12.2. Korzystanie z Pomocy Zdalnej

12.3. Nawiązywanie połączenia pulpitu zdalnego
13. Zarządzanie dyskami
13.1. Dyski wirtualne
13.2. Instalacja systemu na wirtualnym dysku
14. WDS – zdalna instalacja
15. Hyper – V
15.1. Instalacja
15.2. Zarządzanie Hyper-V
16. Windows Server Update Services
17. Bezpieczeństwo danych i komputera
17.1. Windows Backup
17.2. Shadow Copies
17.3. Kilka uwag ogólnych
17.3.1. Polityka haseł
17.3.2. Podmiana logon.scr
17.3.3. Niezabezpieczone serwery wydruku
17.3.4. Best Practices Analyzer
18. Remote Desktop Services
19. Serwer Wydruku
20. Serwer faksów
21. Volume Activation Services
21.1. Instalacja
21.2. Wstępna konfiguracja VA Services
22. Triki
22.1. Wędrujący i wymuszony profil użytkownika
22.2. Dane w chmurze - mapowanie SkyDrive
22.3. GodMode
23. Windows 2016 bez GUI (wersja Core)
23.1. Instalacja wstępna konfiguracja
23.2. Zarządzanie systemem w wersji Core
23.2.1. Interfejsy użytkownika
23.2.2. Podstawowe role serwera
24. Nienadzorowana instalacja Active Directory
25. Migracja z Windows Server 2003
25.1. Podnoszenie Domain Functional Level
26. Instalowanie Active Directory Role na Windows Server 2012

27. Przesyłanie roli Flexible Single Master Operations (FSMO)
28. Zmiana Active Directory Domain Controller
29. Zmiana schematu wzorcowego
30. Dodawanie konsoli schematu Active Directory z MMC
31. Usuwanie serwera z głównego katalogu.
32. Migracja z Windows Server 2008
32.1. Podnoszenie Domain Functional Level
33. Migracja z Windows 2012
34. Weryfikacja poprawności działania usługi katalogowej Active Directory
35. Przeniesienie ról FSMO na nowy kontroler domeny
36. Deinstalacja starego kontrolera domeny
37. Przywracanie usługi Active Directory po katastrofalnej awarii
38. Wykonywanie kopii zapasowej systemu
39. Dodatkowy kontroler domeny
40. Instalacja AD Role na Serwerze
41. Awansowanie serwera na kontroler domeny
42. Dodawanie domeny podrzędnej
Krok 1. Konfiguracja statycznego IP
Krok 2. Dodanie serwera do domeny
Krok 3. Instalacja roli AD
Krok 4. Promocja serwera jako kontrolera domeny
Krok 5. Dodawanie serwera/klienta do subdomeny
43. Klaster awaryjny Hyper-V
44. Migracja na żywo w klastrze Hyper-V
45. Remote FX
45.1. Instalacja i konfiguracja vGPU RemoteFx
46. Relacja zaufania pomiędzy domenami
1. Tworzenie przekazywarki DNS
46.1. Tworzenie TRUST
47. Kontroler domeny tylko do odczytu (RODC)
48. Jak działa uwierzytelnianie użytkownika.
Sprawdzanie przykładu procesu logowania
49. Veeam
49.1. Instalacja VEEAM
49.2. Dodawanie serwera do tworzenia kopii zapasowych

49.3. Tworzenie Backup Job
49.4. Wykonanie pełnego przywracania VM
50. Microsoft Azure
Usługi w chmurze to kolejny model, który wspieramy w budowaniu aplikacji.
Fault Domains
Upgrade Domains
51. Kontenery Docker w Windows Server
51.1. Podstawy kontenerów systemu Windows
Wirtualne Maszyny vs Kontenery
Architektura Wirtualnych Maszyn
Architektura Kontenerów
Kontenery Windows Server vs Kontenery Hyper-V
Docker
Platforma Docker
Kontenery Windows w praktyce
51.2. Image2Docker
Licencjonowanie
Jak to działa?
51.3. Windows Server 2016 z kontenerami na platformie Azure
51.4. Komendy Dockera
51.5. Retrieve Images from Docker Hub
51.6. Wdrażanie nowego kontenera Windows
51.7. Budowanie własnego obrazu kontenera
51.8. Tworzenie obrazu kontenera
51.9. Przesyłanie obrazu do Docker Hub
51.10. Kontenery Linux w systemie Windows: niwelowanie różnic
51.11. Izolacja Hyper-V
52. Chronione maszyny wirtualne w Hyper-V (Shielded VM)
52.1. Komponenty wymagane do skonfigurowania chronionego środowiska VM
52.2. Konfiguracja węzła HGS
52.3. Inicjalizacja węzła HGS
52.4. Konfiguracja kontrolera domeny wykonawcy
52.5. Konfiguracja hosta strzeżonego
53. W jednej z sieci z Mac OS X

53.1. Konfiguracja Magic Triangle

Wstęp

Niniejsza książka stanowi praktyczny przewodnik po Windows Serwer 2016. Stanowi ona propozycję nie tylko dla początkujących administratorów, lecz także dla tych doświadczonych, pragnących szybko i w przyjazny sposób poznać nowości nowego systemu serwerowego firmy Microsoft. Prezentuje najważniejsze jego funkcje i możliwości. Poza niezbędną teorią zawiera szczegółowe instrukcje i ćwiczenia, w których każdy element, nawet najdrobniejszy, jest przedstawiony na zrzucie ekranowym, objaśnionym tak, by osoba, która pierwszy raz pracuje z Windows Serwer, poradziła sobie z jego konfiguracją i administracją. Książka została napisana tak, aby po zapoznaniu się z jej treścią od początku do końca, użytkownikowi udało się w pełni skonfigurować własny serwer, a następnie nadzorować jego działanie i nim administrować. Jest kompatybilna zarówno z anglojęzyczną, jak i polskojęzyczną wersją systemu, która dopiero będzie miała swoją premierę. Wszelkie ewentualne poprawki zostaną opublikowane na blogu autora: http://www.wolk.pl. Z tej publikacji czytelnik nauczy się także współpracować z maszynami i sieciami opartymi na systemach z rodziny Mac OS X oraz Linux. Współdzielenie się zasobami oraz wspólna praca w domenie czy grupie roboczej nie będzie

stanowić dla niego żadnego problemu. Przy okazji czytelnik zapozna się także z zaawansowanymi możliwościami nowego serwera. Książka jest idealną propozycją dla osób mających już dość pozycji encyklopedycznych, a pragnących lektury ukierunkowanej na praktykę i ćwiczenia.

O autorze

Doktor inżynier nauk technicznych w dziedzinie informatyki i bioinformatyki. Pasjonat zagadnień związanych ze sztuczną inteligencją, uczeniem maszynowym, sieciami komputerowymi oraz szeroko pojętymi multimediami. Wykładowca, trener IT, autor książek specjalistycznych a także publicysta internetowy. Certyfikowany specjalista Microsoft, Adobe, Apple, w3schools oraz EITCA. Recenzent konferencji naukowych.

Jego specjalizacja to sztuczna inteligencja, inżynieria lingwistyczna, NLP, aplikacje mobilne, multimedia, aplikacje graficzne Adobe, HTML 5, budowa sieci IT oraz produkty serwerowe firm Apple i Microsoft. Posiada uprawnienia pedagogiczne.

Doświadczony projektant infrastruktur sieciowych dla firm oraz instytucji.

Od 2009 roku redaktor portali informatycznych: in4.pl, pclab.pl oraz własnego bloga: www.wolk.pl, na łamach których opublikował kilkadziesiąt artykułów oraz poradników z dziedziny informatyki. Tworzy także autorskie materiały szkoleniowe, udziela się na portalu e-biotechnologia.pl, a także jest autorem artykułów dla „iCoder Magazine”.

Posiada liczne certyfikaty firm Apple i Microsoft, między innymi Apple Certified System Administrator (ACSA),

Microsoft Certified System Administrator (MCSA) oraz Microsoft Certified IT Professional (MCITP).

Naukowiec i adiunkt w katedrze Multimediów Polsko-Japońskiej Akademii Technik Komputerowych w Warszawie. Prowadzi badania naukowe związane z przetwarzaniem języka naturalnego oraz uczeniem maszynowym opartym na metodach statystycznych oraz sieciach neuronowych. Recenzent specjalistycznych konferencji naukowych oraz branżowych czasopism.

W ramach swojej pracy dydaktycznej prowadzi zajęcia na wydziale Informatyki oraz Sztuki Nowych Mediów w Polsko-Japońskiej Akademii Technik Komputerowych, w przeszłości także prowadził zajęcia dydaktyczne w Warszawskiej Szkole Fotografii i Grafiki Projektowej (przedmioty: grafika komputerowa, multimedia, warsztaty komputerowe I – Photoshop, warsztaty komputerowe II – Adobe AIR [projektowanie aplikacji mobilnych], kompozycja proceduralna – HTML5, CSS3, Javascript, interakcja człowiek–komputer – badanie użyteczności, grafika wektorowa – Ilustrator, magisterska pracownia dyplomowa – tematy mieszane). Był promotorem technicznym prac licencjackich oraz magisterskich na Wydziale Sztuki Nowych Mediów, a także recenzentem na Wydziale Informatyki.

1. Instalacja

Niniejszy rozdział opisuje proces instalacji systemu Windows Server 2016. Można ją wykonać samodzielnie na dowolnym komputerze, lecz w celach ćwiczeniowych zalecana jest instalacja według książki w środowisku wirtualnym przy użyciu wersji testowej Microsoft Windows Server 2016 oraz systemu maszyn wirtualnych VirtualBox. Zaleca się także wykonywanie częstych migawek maszyny wirtualnej, np. przed instalacją kolejnych ról serwera – pozwoli to w razie błędu w konfiguracji szybko przywrócić maszynę do stanu poprzedniego.

Windows Server 2016 występuje w trzech edycjach:

⇒ Essentials – jest idealna dla małych przedsiębiorstw z podstawowymi wymaganiami względem IT; bardzo mały lub brak działu IT. Uprawnienia do wirtualizacji: brak; jedna instalacja, fizyczna lub wirtualna. Model licencjonowania oparty na CPU. Licencje CAL nie są wymagane (ograniczenie do 25 użytkowników/50 urządzeń). Limit pamięci RAM 64 GB, a CPU 2.

⇒ Standard – przeznaczona dla przedsiębiorstw, które wymagają zaawansowanych funkcji lub są zwirtualizowane w minimalnym stopniu. Uprawnienia do wirtualizacji to 2 wirtualne maszyny lub 2 kontenery Hyper-V. Model

licencjonowania oparty na rdzeniach, licencje CAL są wymagane. Limit pamięci RAM 24 TB, a CPU 512 rdzeni.

⇒ Datacenter – dla wszystkich wysoko zwirtualizowanych przedsiębiorstw z dużymi wymaganiami względem IT. Nieograniczona ilość wirtualnych maszyn lub kontenerów Hyper-V. Model licencjonowania oparty na rdzeniach, licencje CAL są wymagane. Limit pamięci RAM 24 TB, a CPU 512 rdzeni. Na tej wersji systemu została oparta niniejsza książka.

Edycje systemu Windows Server 2016 różnią się pod względem dostępnych ról i usług serwera:

Rola serwera	Datacenter/Standard	Essentials
Usługi certyfikatów Active Directory	✓	✓ automatycznie zainstalowane / skonfigurowane (1)
Usługi domenowe Active Directory	✓	✓ automatycznie zainstalowane / skonfigurowane (2)
Usługi Active Directory Federation Services	✓	✓
Usługi LDS Active Directory	✓	✓

Usługi Active Directory Rights Management [3]	✓	✓
Serwer aplikacji	✓	✓
Serwer DHCP	✓	✓
Serwer DNS	✓	✓ **automatycznie zainstalowany / skonfigurowany**
Serwer faksów	✓	✓
Usługi plików i magazynowania	✓	✓ **automatycznie zainstalowane / skonfigurowane [4]**
Funkcja Hyper-V	✓	✓
Usługi zasad sieciowych i dostępu sieciowego	✓	✓ **automatycznie zainstalowane / skonfigurowane**
Usługi drukowania i zarządzania dokumentami	✓	✓
Dostęp zdalny	✓	✓ **automatycznie zainstalowany / skonfigurowany [5]**

Usługi pulpitu zdalnego (6)	✓	**brak**
Usługi aktywacji zbiorczej	✓	✓
Usługi sieci Web (IIS)	✓	**✓ automatycznie zainstalowane / skonfigurowane**
Usługi wdrażania systemu Windows	✓	✓
Program Windows Server Update Services	✓	✓

(1) Funkcja ograniczona do konfiguracji jednostek certyfikacyjnych – inne funkcje Active Directory Certificate Services (Network Device Enrollment Services, Online Responder Service) są niedostępne. Więcej informacji można znaleźć na stronach TechNet, w opisie roli AD CS.

(2) Musi być rootem w strukturze domeny AD DS i pełnić wszystkie główne role operacyjne.

(3) Dostęp wymaga dodatkowej licencji AD RMS CAL.

(4) Deduplikacja danych nie jest dostępna.

(5) Ograniczenie do 50 połączeń RRAS i 50 połączeń IAS; DirectAccess i VPN są wspierane.

(6) Dostęp wymaga dodatkowych licencji RDS CAL (wyjątek: wykorzystanie funkcji Remote Web Access w edycji Essentials).

(7) Tylko usługa RD Gateway jest zainstalowana i skonfigurowana, pozostałe zdalne usługi (włączając w to host sesji RD) nie są wspierane.

Edycje systemu Windows Server 2016 różnią się pod względem dostępnych funkcjonalności:

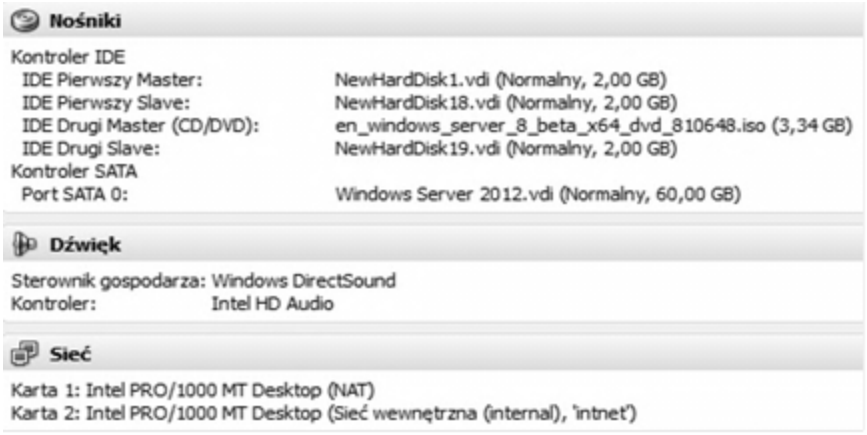
Funkcjonalność	Essentials	Standard	Datacenter
Podstawowe funkcjonalności w Windows Server	**brak**	✓	✓
Kontenery OSEs / Hyper-V	**Brak**	✓ **2**	✓ **bez ograniczeń**
Kontenery Windows Server	**Brak**	✓ **bez ograniczeń**	✓ **bez ograniczeń**
Host Guardian Service	**Brak**	✓	✓
Nano Server	**Brak**	✓*	✓*
Funkcjonalności storage z Storage Spaces Direct i Storage Replica	**Brak**	**Brak**	✓
Shielded Virtual Machines	**brak**	**brak**	✓
Networking stack	**brak**	**brak**	✓

* Instalacja systemu Nano Server i jego eksploatacja wymaga Software Assurance.

1.1. Wymagania sprzętowe i opis środowiska

W tym dziale zajęto się dość prostym zagadnieniem, jakim jest instalacja systemu. Do tego celu będzie potrzebny komputer lub wirtualna maszyna z procesorem wspierającym architekturę x64 taktowany zegarem minimum 1,4 GHz, z 512 MB pamięci RAM oraz minimum 32 GB wolnego miejsca na dysku. W praktyce zaleca się użycie minimum dwurdzeniowego procesora, 4 GB pamięci RAM oraz dużego i szybkiego dysku. W komputerze potrzebne też będą dwie karty sieciowe. Jedna podłączona do sieci lokalnej, a druga do globalnej. Tworząc wirtualne środowisko zadbano o to.

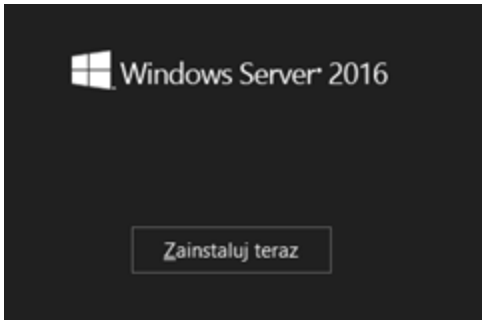
Stworzono też trzy wirtualne dyski twarde. Nie są one wymogiem. Zdecydowano się na nie w celu dalszego zaprezentowania pracy na macierzach dyskowych.



1.2. Proces instalacji

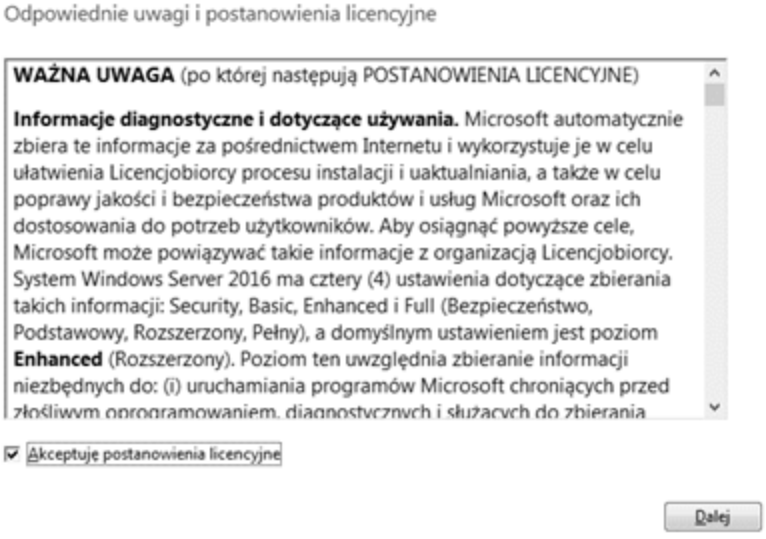
Instalator systemu wygląda bardzo podobnie do tego znanego z Windows 7 i Windows Vista. Do zaprezentowania kolejnych kroków została użyta testowa wersja systemu Windows Server 2016 RC dostępna do pobrania na stronach Microsoft. Po uruchomieniu komputera z płyty CD, USB lub PXE po chwili pojawi się ekran powitalny. Należy ustawić preferencje systemowe i nacisnąć przycisk Dalej (Next).

Na kolejnej planszy należy kliknąć przycisk Zainstaluj teraz (Install Now).

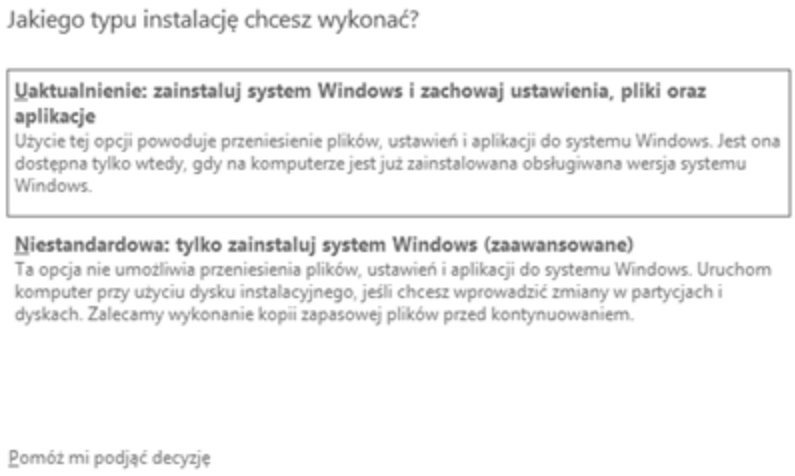


W kolejnym oknie instalatora należy wybrać wersję systemu Windows, na którą została zakupiona licencja.

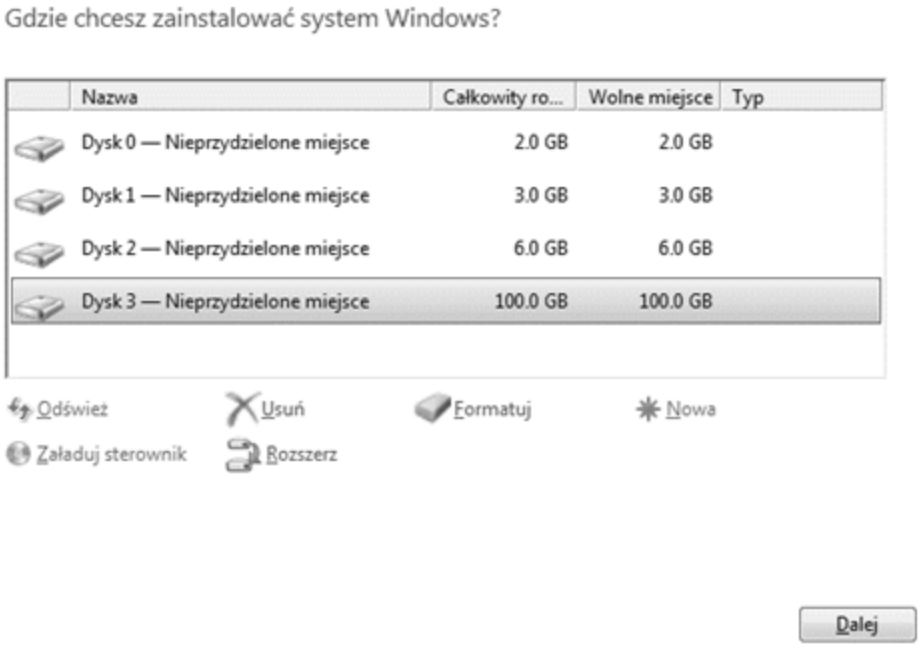
W następnym kroku należy zaakceptować umowę licencyjną i kliknąć przycisk **Dalej (Next).**



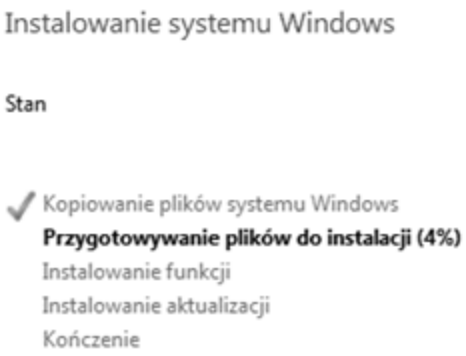
Jako że przygotowywana jest nowa instalacja, należy wybrać opcję niestandardową, czyli zaawansowaną **(Install Windows only (advanced)).**



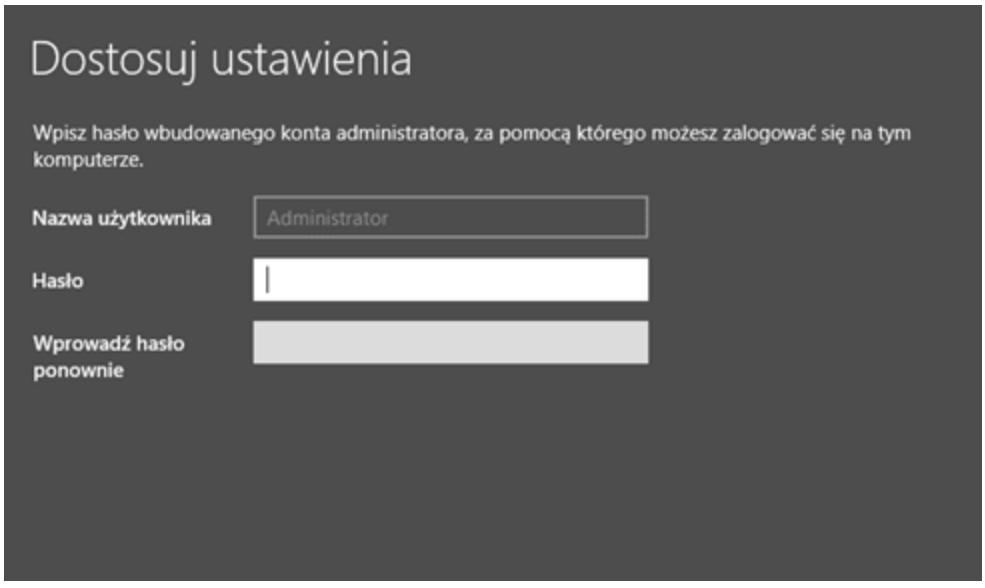
Pojawi się ekran wyboru dysku, na którym ma zostać zainstalowany system operacyjny. W tym przypadku zostanie zaznaczony Dysk3, a następnie należy kliknąć przycisk Dalej (Next). Drzewo partycji utworzy się automatycznie.



Rozpocznie się proces instalacji, którego czas trwania będzie zależny od wydajności komputera, na którym się on odbywa.



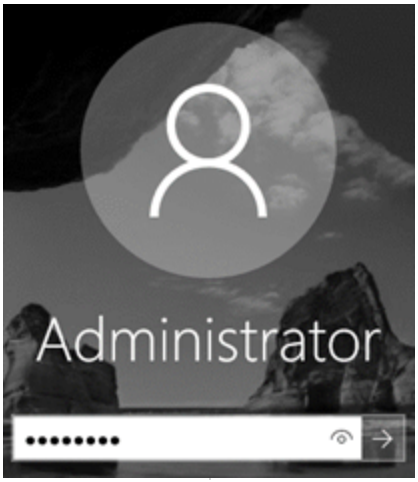
Po wgraniu wszystkich plików, podczas pierwszego uruchomiania komputer poprosi o zmianę hasła dla konta administratora. Należy dwukrotnie wprowadzić hasło, a następnie kliknąć przycisk Zakończ (Finish). Hasło musi spełniać odpowiednie normy bezpieczeństwa, tj. musi mieć minimum 7 znaków, w tym jedną dużą literę, jedną cyfrę i jeden znak specjalny, jak np. @ lub !.



Pojawi się ekran logowania. Aby się zalogować należy na klawiaturze wcisnąć kombinację klawiszy **Ctrl+Alt+Del/Delete.**

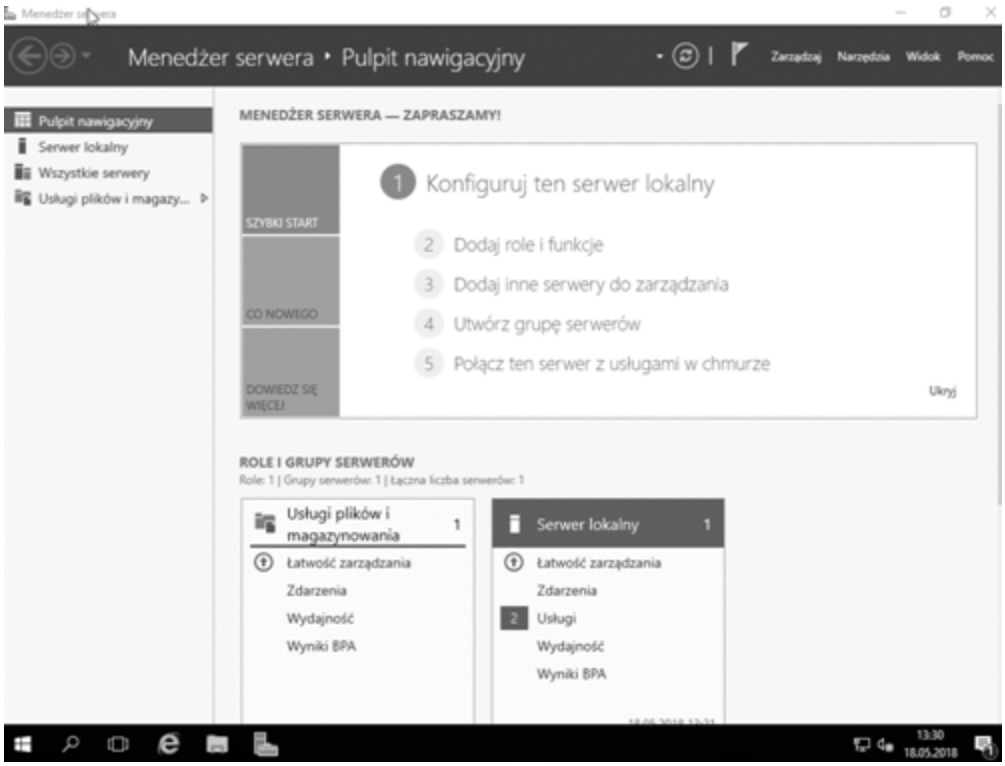
W oknie, które zostanie wyświetlone, należy podać hasło dla pożądanego użytkownika, a następnie kliknąć ikonkę

tuż obok pola wpisywania hasła.



Po zalogowaniu wczyta się całkowicie nowy interfejs użytkownika, znany z systemu Windows 10. System

Windows Server 2016 jest już zainstalowany, a naszym oczom ukazał się menadżer serwera!



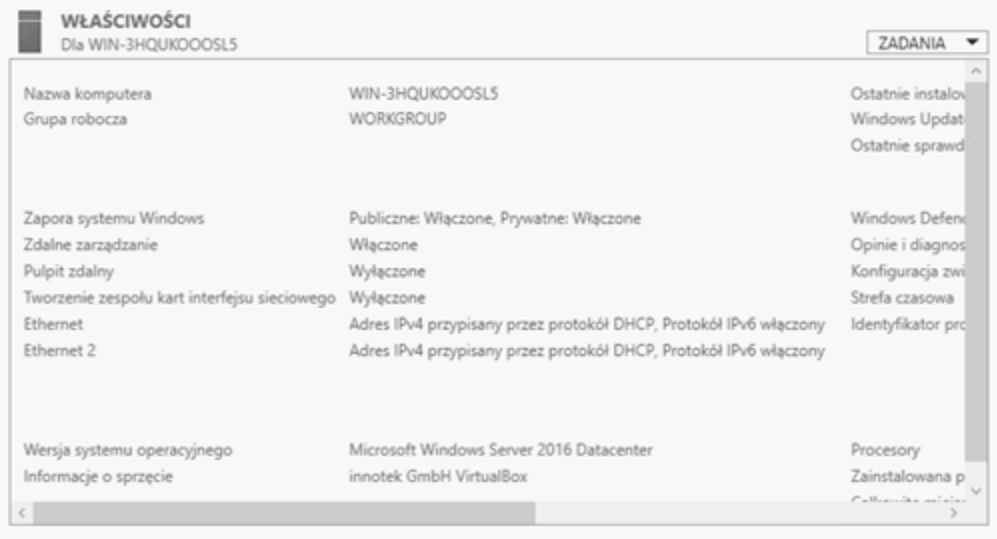
2. Post-instalacja

Po pomyślnym uruchomieniu serwera, zanim przejdzie się do jego dalszej konfiguracji, należy wykonać kilka ważnych czynności. Przede wszystkim zapoznać się z zupełnie nowym interfejsem użytkownika i zmienioną konsolą Menadżera Serwera względem wcześniejszych wersji. Następnie zaktualizować serwer, skonfigurować interfejsy sieciowe i przygotować maszynę do awansu na kontroler domeny.

2.1. Czynności post-instalacyjne

Kiedy na komputerze zainstalowane są już wszystkie urządzenia, można spokojnie przystąpić do podstawowej jego konfiguracji. Z pomocą przychodzi **Konsola Zarządzania Serwerem (Server Manager)**, która w swoim głównym oknie prezentuje cztey podstawowe kroki. Pierwszym z nich jest konfiguracja serwera lokalnego.

Po wybraniu opcji Konfiguruj Serwer Lokalny (Configure this local server) włączona zostanie konsola, w której można zmienić nazwę komputera, przyłączyć go do grupy roboczej, a także zarządzać aktualizacjami, firewallem, raportowaniem błędów, ustawieniami sieci, zwiększonymi zabezpieczeniami IE itp.

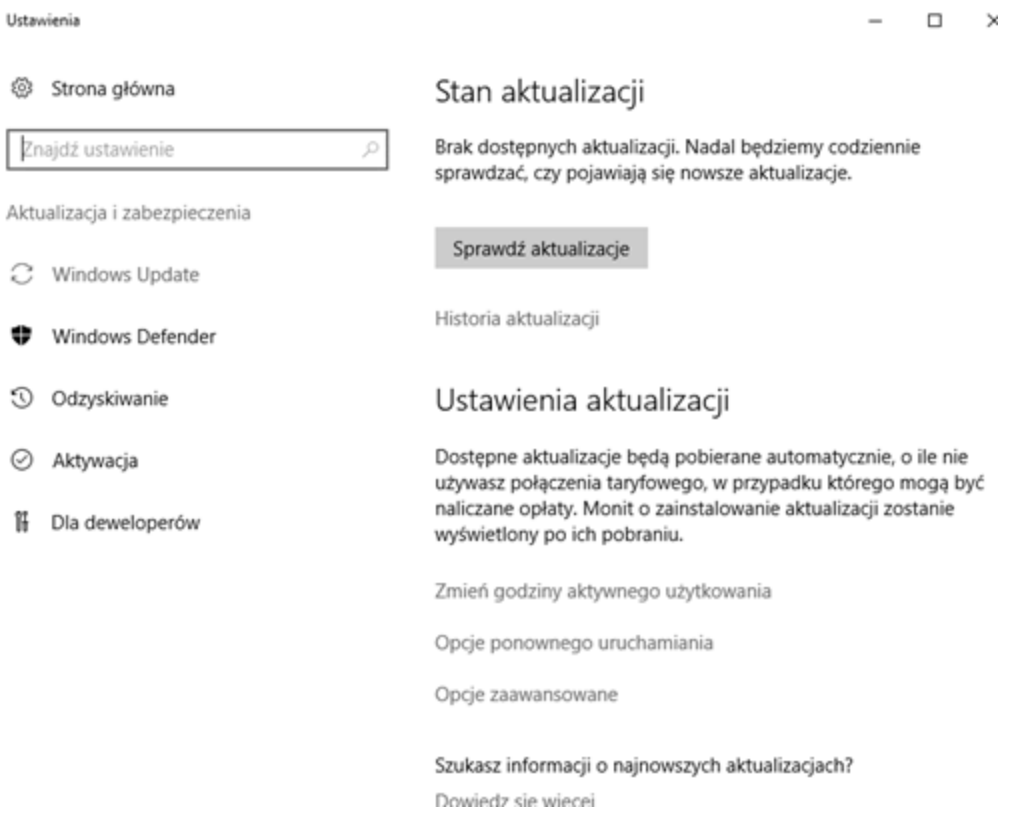


2.1.1. Aktualizacje

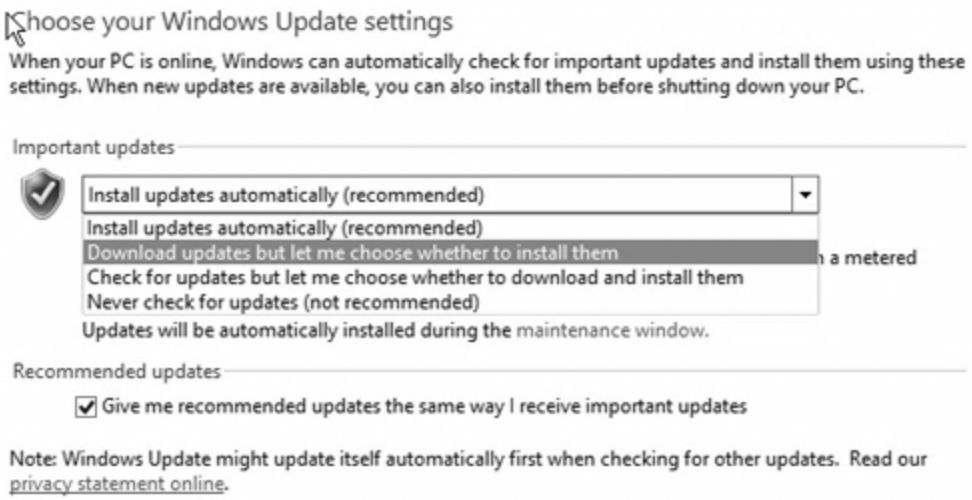
W pierwszej kolejności warto uruchomić aktualizacje automatyczne i zainstalować wszystkie dostępne aktualizacje, używając przycisku **Włącz automatyczne aktualizacje (Turn on automatic updates).**

Kiedy system zostanie przeanalizowany, można rozpocząć aktualizację, klikając przycisk **Zainstaluj Aktualizacje (Install Updates).**

W menu po lewej stronie należy wybrać opcję Zmień Ustawienia **(Change Settings)**.



W oknie, które się pojawi, najwygodniej będzie wybrać opcję pierwszą – **Zainstaluj aktualizacje automatycznie (Install updates automatically)**. Jeśli jednak na celu jest uniknięcie samoistnych instalacji aktualizacji, a co za tym idzie ponownych uruchomień komputera, należy wybrać opcję drugą – Pobierz aktualizacje, ale daj mi wybrać kiedy zostaną zainstalowane **(Download updates but let me choose whether to Install them)**, która jest w przypadku serwera znacznie bezpieczniejsza dla zachowania ciągłości pracy. Następnie należy kliknąć **OK.**

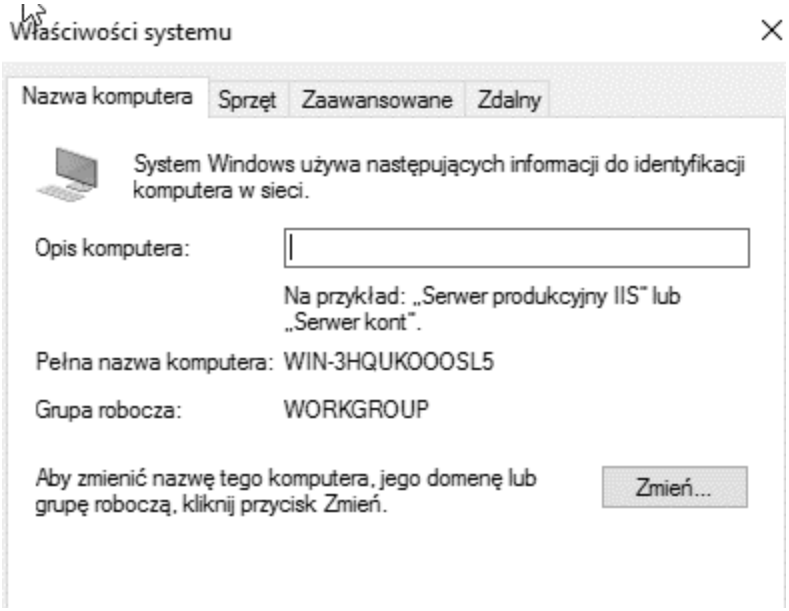


Przed dalszą lekturą i administracją prawdziwym serwerem warto zawsze zaraz po instalacji wykonać aktualizację systemu oraz wgrać najnowsze wersje programów i sterowników, np. przy pomocu programu Driver Booster.

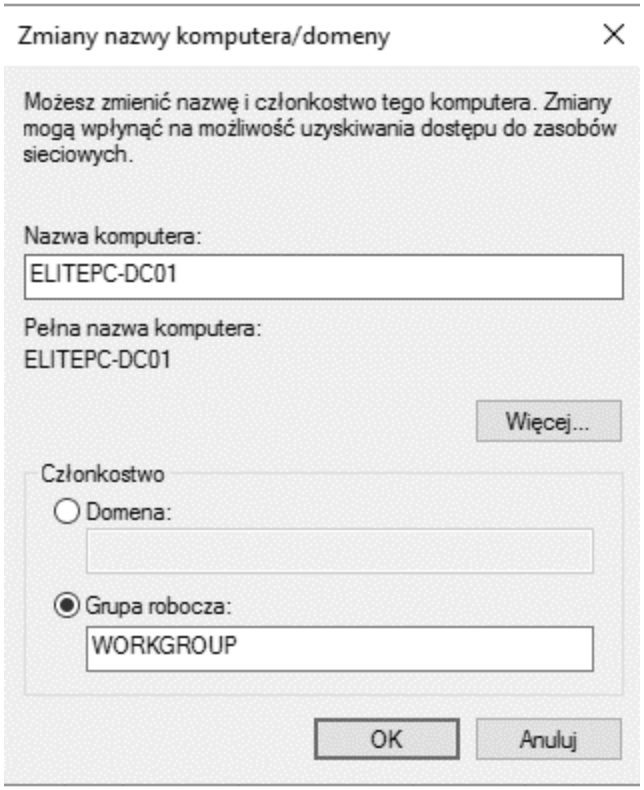
2.1.2. Zmiana nazwy komputera

Na ekranie podsumowującym **Menadżera Serwera (Server Manager)**, w sekcji **Właściwości (Properties)** znajduje się parametr **Nazwa Komputera (Computer Name)**, gdzie należy kliknąć w nazwę komputera.

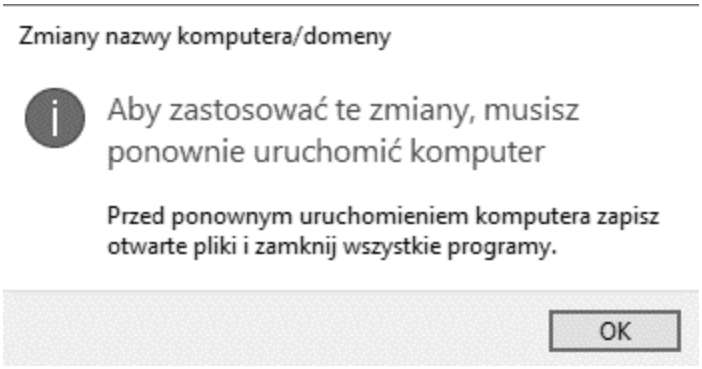
W karcie **Nazwa Komputera (Computer Name)** należy kliknąć przycisk Zmień **(Change)**.



Lepiej na początku ustalić sobie sposób nazewnictwa komputerów, aby utrzymać porządek w sieci, np. ElitePC-DC01, gdzie ElitePC to nazwa firmy, DC – Kontroler Domeny (Domain Controler), a 01 to numer komputera. Zamiennie do DC w nazewnictwie można użyć skrótów SR dla oznaczenia serwera oraz WS (Work Station) dla stacji roboczych.



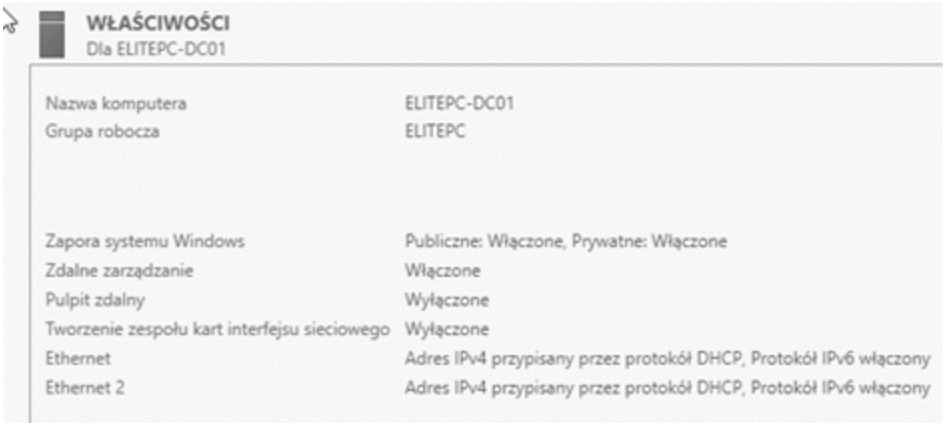
W komunikacie, który się pojawi, należy kliknąć przycisk OK i uruchomić ponownie komputer.



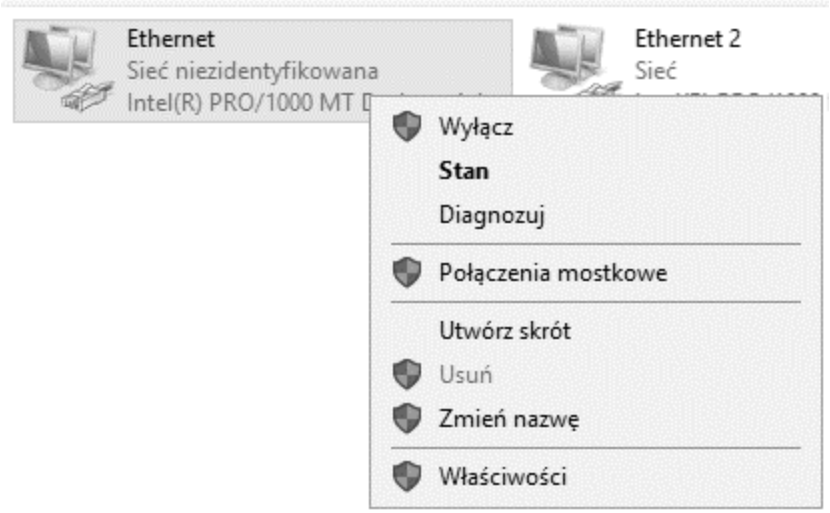
2.2. Konfiguracja sieci

Kolejnym krokiem będzie zmiana nazw interfejsów sieciowych tak, aby w każdej chwili wiedzieć, czy operuje

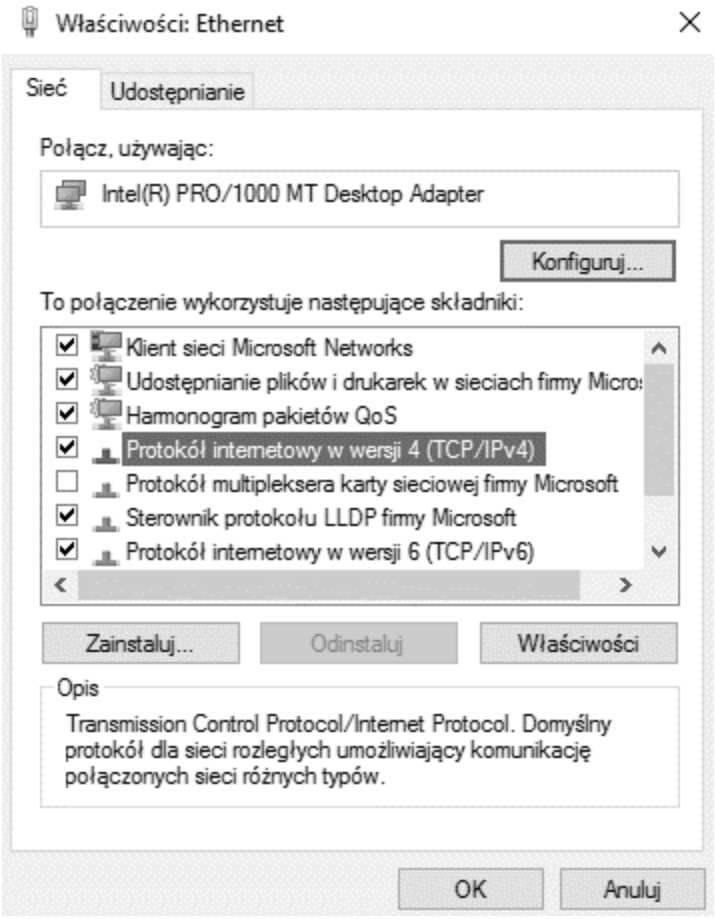
się na łączu internetowym czy też lokalnym. Połączenie z Internetem warto nazwać WAN, a z sieć lokalną LAN. Wystarczy kliknąć na wybranym połączeniu w konsoli zarzadzania serwerem.



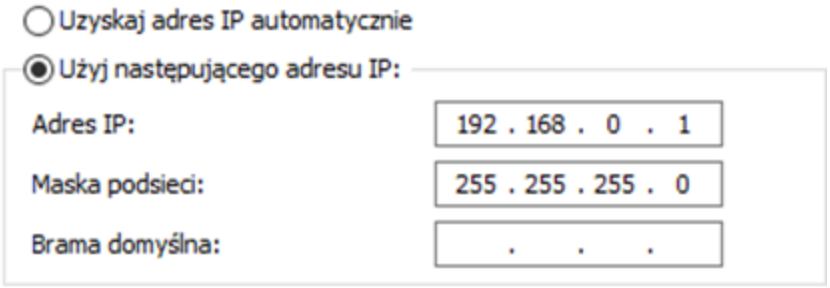
Na karcie sieciowej podpiętej do Internetu należy kliknąć prawym guzikiem i wybrać opcję **Zmień nazwę (Rename)**. Tą samą czynność należy powtórzyć dla drugiej karty sieciowej.



Przy interfejsie łączącym z siecią lokalną należy wejść we Właściwości (Properties) i ustalić stały adres IP, ponieważ chodzi tu o serwer. Należy wejść we Właściwości protokołu IPv4.



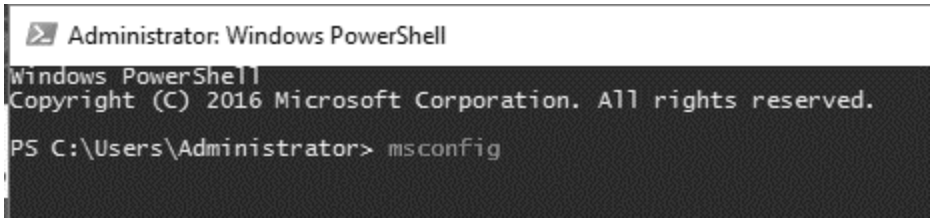
Należy wprowadzić adresy IP z dowolnego zakresu, np. standardowa adresacja 192.168.1.1 przy masce 255.255.255.0.



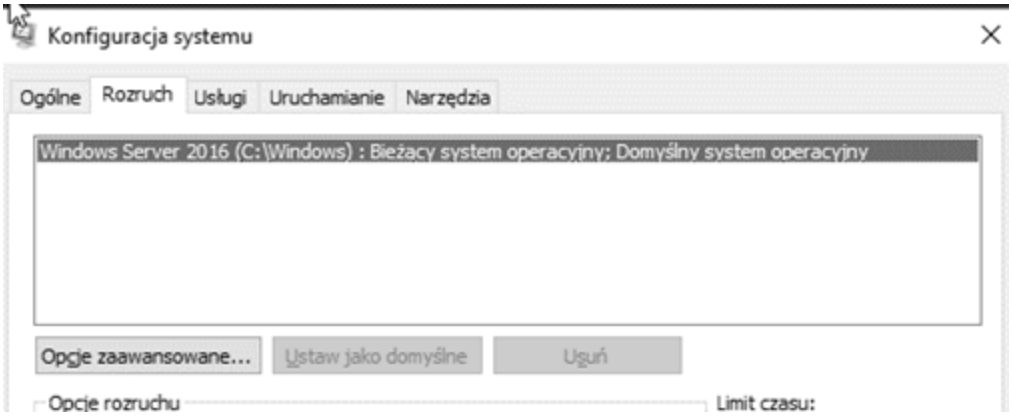
2.3. Zarządzanie procesorami i pamięcią operacyjną

Ostatnim krokiem post-instalacyjnym będzie uruchomienie większej liczby rdzeni procesora podczas startu systemu. W tym celu należy kliknąć na ikonę

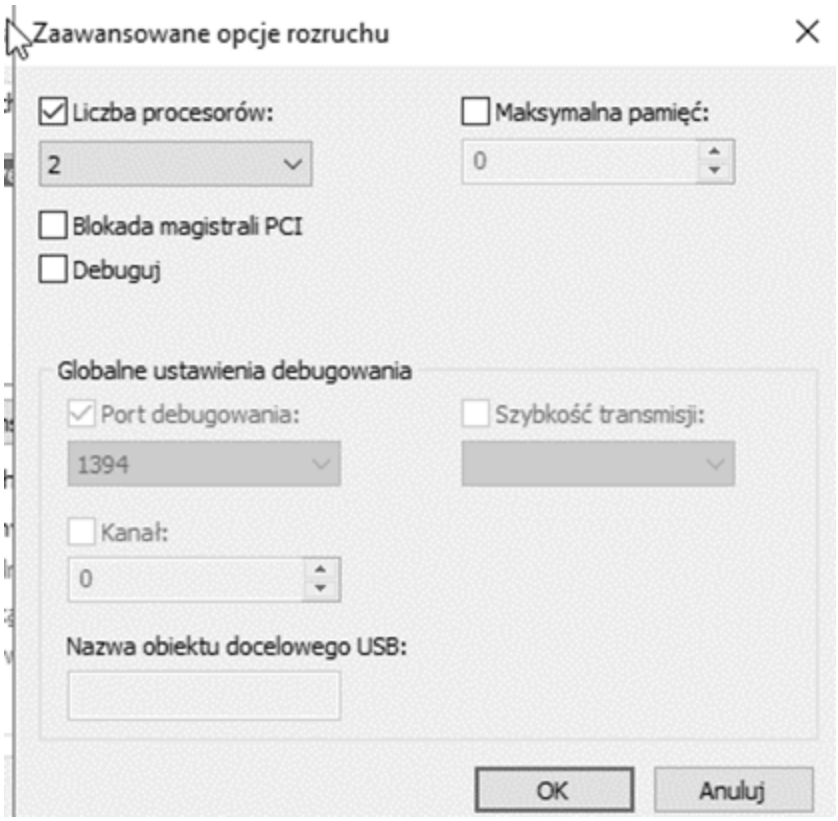
paska Start, związaną z konsolą **Power Shell** i wydać polecenie **msconfig.**



W zakładce **Rozruch (Boot)** konieczne jest kliknięcie **Opcji Zaawansowanych (Advanced options)**.



W następnej kolejność należy zaznaczyć opcję **Liczba procesorów (Number of processors)**, a z rozwijanej listy wybrać ich tak dużo, jak to jest tylko możliwe.



3. Active Directory Domain Services

Usługi Domenowe Active Directory (Active Directory Domain Services) są niezbędne do awansu serwera na główny kontroler domeny. Serwer stanie się w ten sposób centralną bazą danych użytkowników, odpowiedzialnych za autentykację i autoryzację użytkowników. Zostaną wyjaśnione takie pojęcia jak grupa robocza oraz domena. Czytelnik zrozumie, w jakim celu wdraża się domenę, a także na czym polega struktura drzewa oraz lasu. W następnej kolejności prześledzi proces instalacji pierwszego kontrolera domeny i nauczy się zarządzać

obiektami przechowywanymi w Active Directory za pomocą konsoli **Active Directory Users and Computers oraz Active Directory Administrative Center**.

3.1. Czym jest domena?

Na początku warto wyjaśnić kilka pojęć. Przede wszystkim, czym jest domena oraz dlaczego się ją stosuje zamiast grup roboczych. Dla przykładu w grupie roboczej lista kont użytkowników, uprawnienia użytkowników i zabezpieczenia systemu przechowywane są lokalnie, tzn. osobno na każdym komputerze wchodzącym w skład grupy roboczej. Każdy komputer jest jednostką autonomiczną. Aby móc pracować na komputerze należącym do grupy roboczej, trzeba mieć konto na tym komputerze. Wiąże się to z tym, że osób pracujących na jednym komputerze może być więcej, co oznacza konieczność powielania kont na różnych komputerach. To samo dotyczy ustawień i oprogramowania. Co więcej, jeśli ktoś zachowa jakiś plik na jednym komputerze, to nie otworzy go już na innym, chyba że ręcznie go przekopiuje.

Można wyobrazić sobie sytuację, w której zarządza się kilkunastoma komputerami i należy aktualizować programy, zakładać konta nowym pracownikom itp. Byłaby to strasznie żmudna praca. W domenie natomiast zarządzanie informacją o kontach użytkowników, komputerach domeny

oraz zasadach obowiązujących w domenie jest scentralizowane. Komputery współdzielą bazę danych kont, zasad, zabezpieczeń, która znajduje się na kontrolerach domeny. W trakcie logowania się na konto w domenie Windows, dane użytkownika porównywane są z danymi zapisanymi w kontrolerze domeny. Przestaje mieć znaczenie, z którego konkretnie komputera loguje się dany użytkownik, gdyż i tak zachowa swoje pliki i ustawienia.

W przypadku instalacji nowego oprogramowania wystarczy, że administrator wyda taką „dyspozycję" na serwerze, a komputery podłączone do domeny same sobie poradzą z instalacją. Naturalnie logowanie na lokalne konta użytkowników, tak jak to miało miejsce w przypadku grupy roboczej, dalej jest możliwe. To oczywiście tylko czubek góry lodowej, inne możliwości zostaną przedstawione w kolejnych rozdziałach.

Obecnie rozróżnia się dwa typy domen: NT4 oraz Active Directory, której będzie poświęcone najwięcej uwagi. Active Directory to usługa katalogowa będąca implementacją protokołu LDAP. Jest następcą NT4 i usuwa największe wady poprzednika. Wprowadzono do niej hierarchiczność przechowywania informacji, dużo wyższe limity przechowywania informacji (powyżej 1 miliona obiektów w domenie Active Directory) oraz rozszerzalność schematu zawierającego definicje obiektów.

Domeny zorganizowane są hierarchicznie, tworząc strukturę drzewa. Drzewo posiada zawsze przynajmniej jedną domenę – domenę najwyższego poziomu (ang. root)

– korzeń drzewa. Pozostałe domeny (o ile istnieją) mogą być umieszczone poniżej domeny najwyższego poziomu, tworząc drzewo. Takie rozwiązanie często stosuje się w przypadku kilku siedzib firmy lub do wygodnego zarządzania komputerami w dwóch odległych od siebie miejscach. Jako przykład pokazano poniżej fragment drzewa dla firmy ElitePC.

Każde drzewo należy do jakiegoś lasu, każdy las składa się z przynajmniej jednego drzewa. Nie ma możliwości utrzymywania drzewa bez utrzymywania lasu.

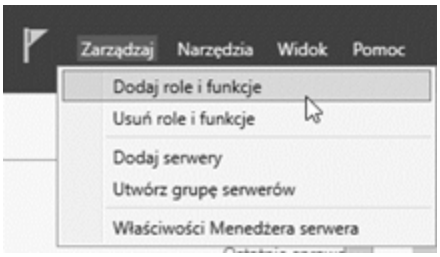
Uwaga!

To odnosi się również do domeny Active Directory – domena nie może istnieć samodzielnie, musi istnieć w jakimś drzewie i jakimś lesie. Jeżeli jest to pierwsza domena, to tworzy pierwsze drzewo (którego korzeniem się staje) oraz pierwszy las. Poniżej przykład lasu z dwoma drzewami:

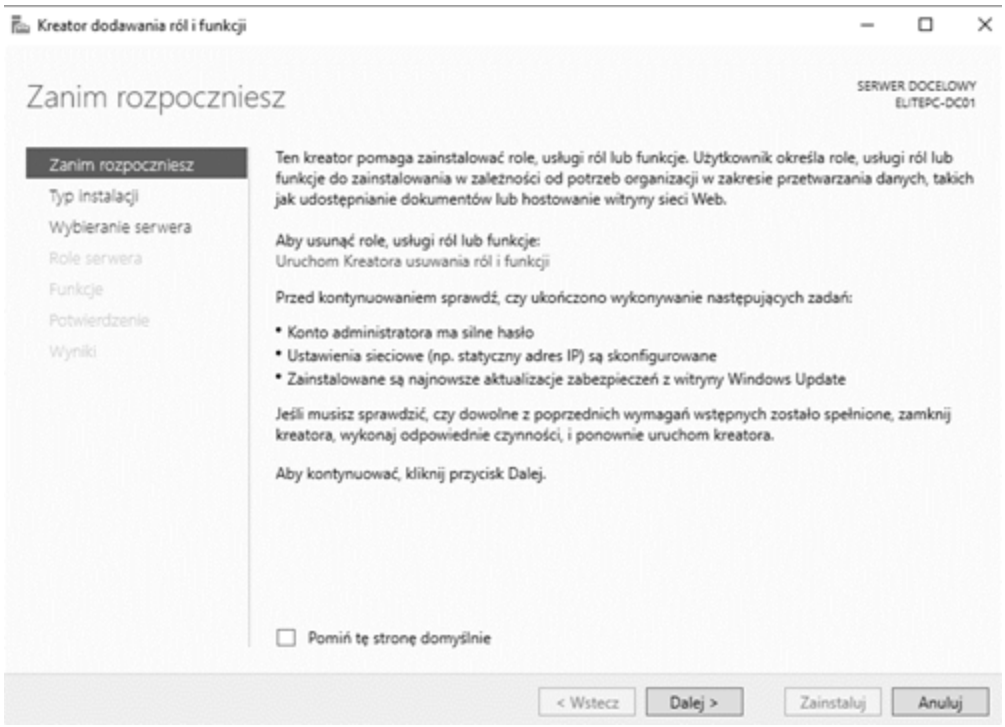
3.2. Instalacja Active Directory Domain Services

W przypadku gdy serwer jest kierowany ku zastosowaniom domowym czy małej firmy, wystarczy jedna domena. Aby rozpocząć instalację, należy kliknąć ikonkę **Menadżer Serwera (Server Manager)** znajdującą się obok guzika **Start**. Warto zapamiętać ten krok, gdyż będzie on często wykonywany.

W **Menadżerze Serwera (Server Manager)** będą instalowane praktycznie wszystkie role dostępne w Windows Serwer 2016.

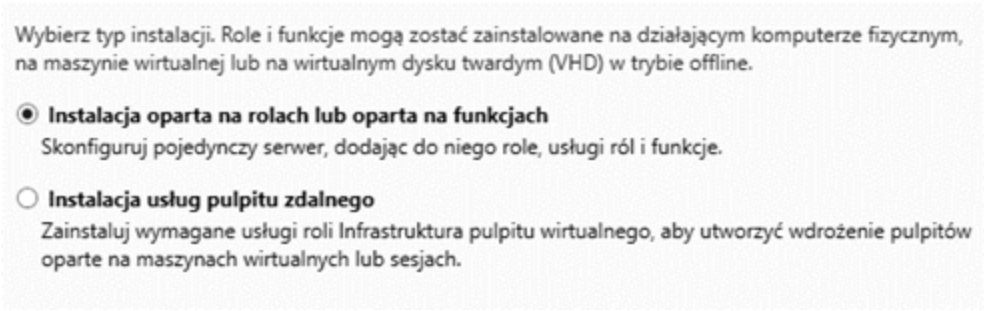


W górnym menu po prawej stronie należy kliknąć w przycisk Zarządzaj **(Manage)**, a następnie wybrać opcję Dodaj role i funkcje **(Add Roles and Features)**. Pojawi się plansza powitalna, gdzie konieczne jest kliknięcie w przycisk Dalej **(Next)**.

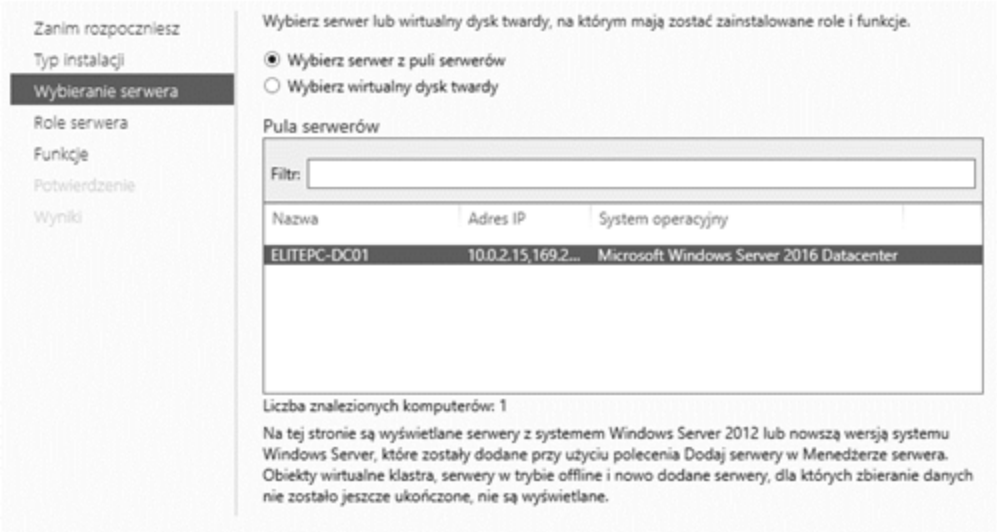


Jedną z nowości Windows Server 2016 jest możliwość instalowania ról serwera na zdalnych komputerach, obrazach dysków VHD czy na maszynach wirtualnych. Na potrzeby tej publikacji i dla ułatwienia zrozumienia omawianych zagadnień na razie będą instalowane wszelkie nowe role i funkcje na tej samej maszynie. Należy wybrać więc opcję pierwszą Role-based i kliknąć **Dalej (Next)**.

Instalacja oparta na scenariuszu jest nowością w systemie Windows Server 2016. Dzięki niej można jednocześnie instalować komponenty związane z **Usługami Pulpitu Zdalnego (Remote Desktop Services)**. AD jest instalowane jako klasyczna rola.

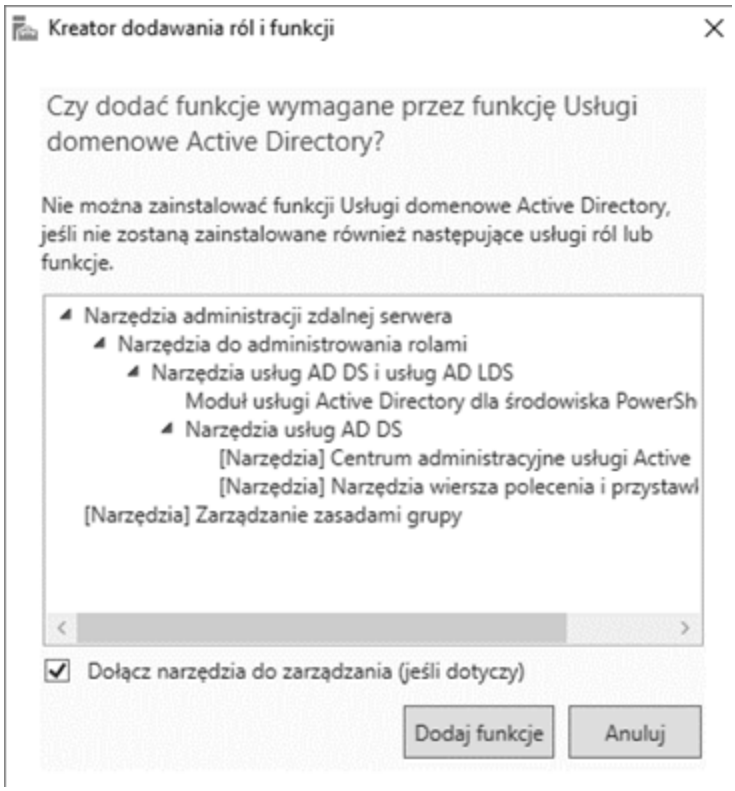


W kolejnym kroku należy wybrać serwer, na jakim dana rola ma zostać skonfigurowana. Naturalnie w środowisku przykładowym do wyboru jest tylko jedna maszyna. Należy ją zaznaczyć i wybrać przycisk **Dalej (Next)**. Jest to kolejna z nowości w systemie Windows Server 2016. Pozwala ona zdalnie instalować role na innych serwerach, a także je wgrywać na wirtualne dyski VHD, które można potem podmontować pod konkretny serwer.

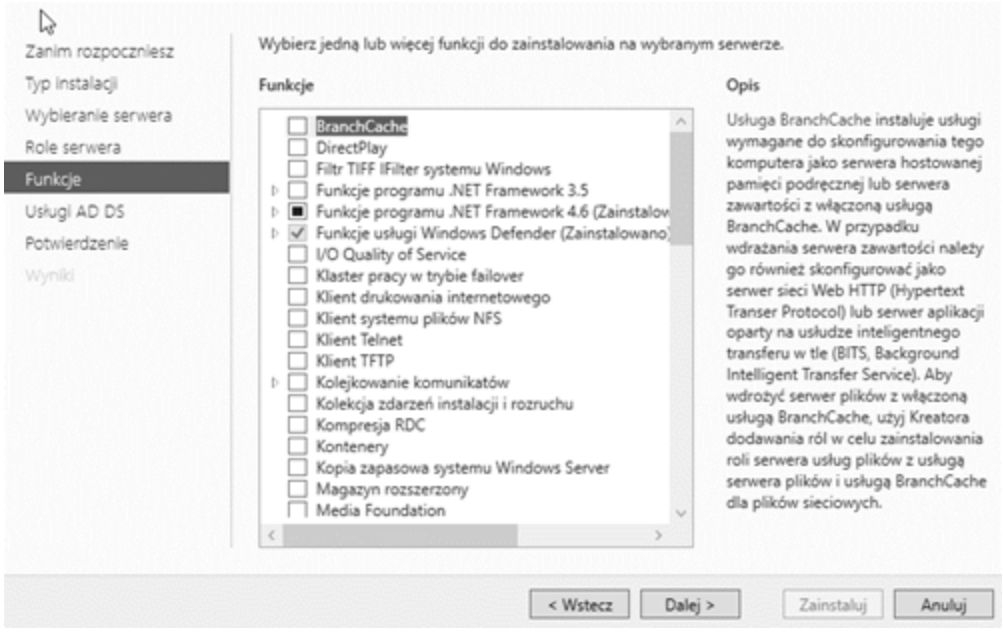


Następnie należy wybrać Usługi Domenowe w **Usłudze Active Directory** (**Active Directory Domain Services**). Znawcy tematu zauważą, że Role są niemalże identyczne z tymi z Windows Server 2008 R2. Nowością jest Zdalny **Dostęp (Remote Access)**, który w rzeczywistości jest nową nazwą dla Direct Access oraz Usługi Aktywacji Woluminowej (Volume Activation Services) związane z aktywacją licencji woluminowych.

Pojawi się komunikat, na którym należy kliknąć **Dodaj Wymagane Funkcje (Add Features)**, a następnie **Dalej (Next).**

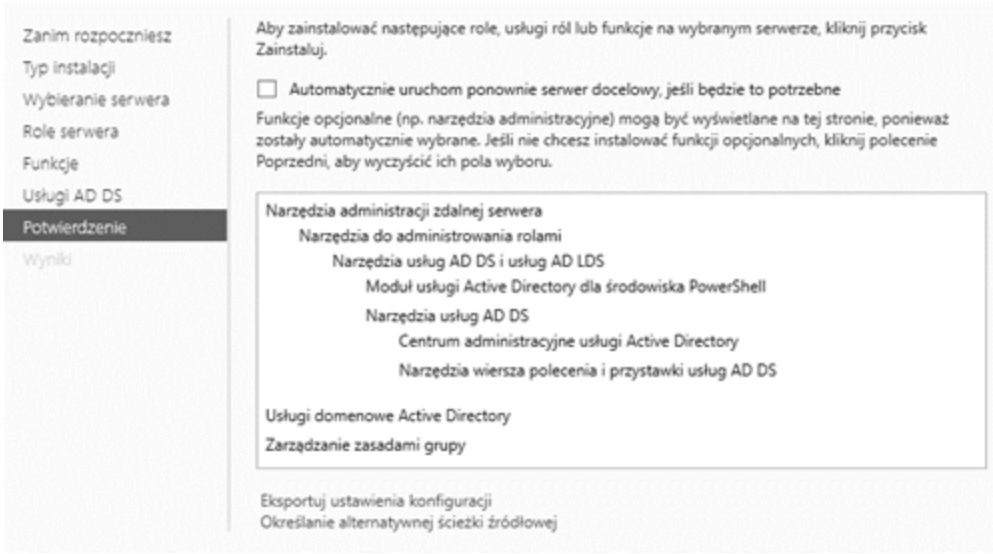


Następnie ponownie należy kliknąć w przycisk Dalej (Next).

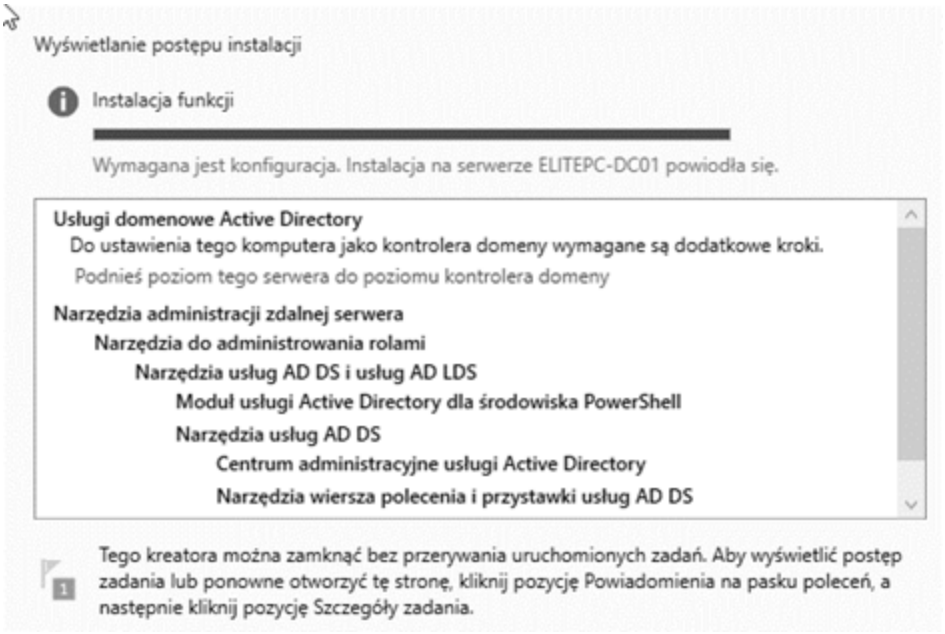


Poniższe okno prezentuje informacje podsumowujące oraz dotyczące dalszych kroków instalacyjnych. Między innymi powiadamia ono o konieczności zainstalowania serwera DNS, ponieważ ta rola jest wymagana do prawidłowego działania AD. Wgrany zostanie także komponent odpowiadający za replikację serwera DFS, który został wprowadzony już w Windows 2003 R2 do replikacji wolumenu SYSVOL. Po raz kolejny należy kliknąć w Dalej (Next).

Na ostatniej już planszy należy wybrać przycisk Zainstaluj (Install).



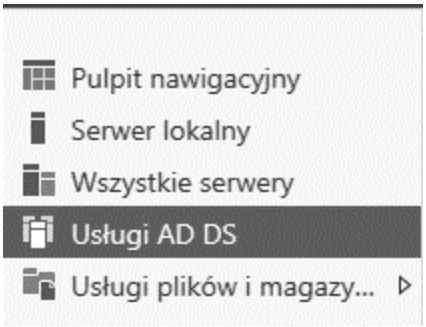
Proces instalacji chwilę potrwa. Gdy dobiegnie końca, należy kliknąć w Zakończ (Close).



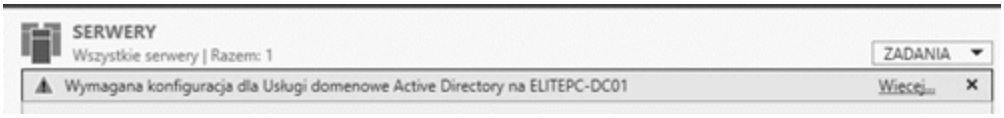
Aby instalacja dobiegła końca, należy ponownie uruchomić komputer.

3.3. Wstępna konfiguracja AD DS

W Menadżerze Serwera (Server Manager) w menu po lewej stronie należy kliknąć w Usługi Domenowe w Usłudze Active Directory (AD DS).

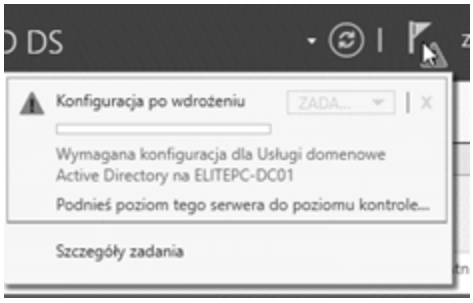


Kiedy plansza się załaduje, po prawej stronie pojawi się wyróżniony napis Więcej (More), który należy wybrać.

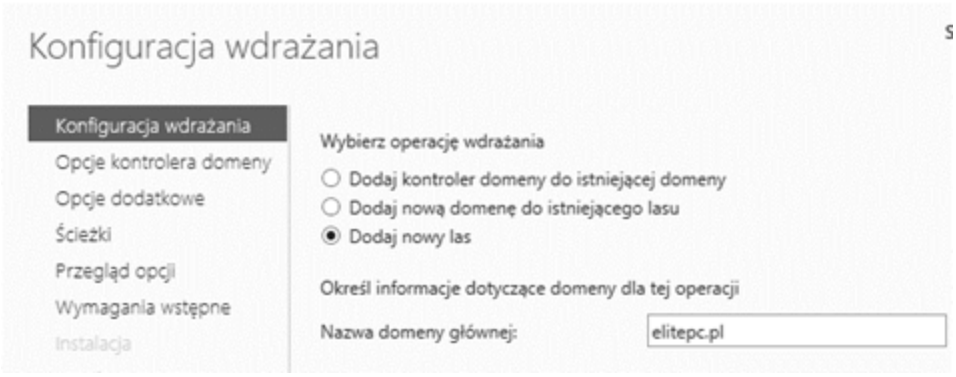


Następnie należy wybrać Promuje ten serwer na kontroler domeny (Promote this server to a domain Controller) poprzez wybranie odpowiedniej akcji.

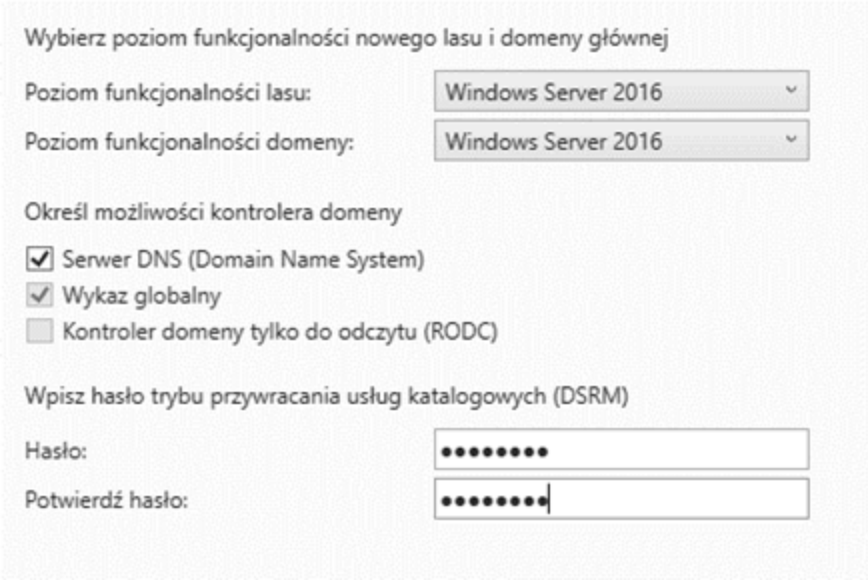
To samo można uzyskać, korzystając bezpośrednio z menu akcji, które oznaczone jest w górnym menu chorągiewką.



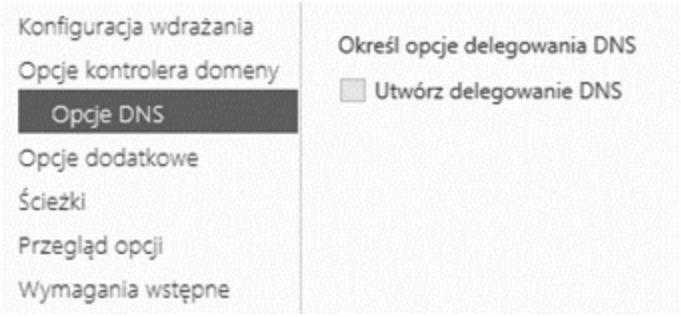
Ponieważ tworzony jest pierwszy serwer, który jednocześnie będzie głównym kontrolerem domeny w sieci, należy wybrać opcję trzecią. W przeciwnym wypadku, kiedy serwer miałby zostać wpięty do istniejącej już struktury, konieczne byłoby wybranie opcji drugiej lub pierwszej. Niezbędne jest także podanie nazwy domeny, która ma zostać stworzona.



Należy ustawić poziom funkcjonalności lasu tak, aby był kompatybilny z resztą sieci. Jeżeli istniałby już jakiś kontroler domeny, pracujący pod kontrolą Windows Server 2003, musiałby zostać wybrany taki sam poziom. Wiązałoby się to niestety z utratą nowych funkcjonalności wprowadzonych w Windows Server 2016. W przypadku przedstawionym w książce należy wybrać poziom najwyższy, czyli Windows Server 2016. Przy okazji zostanie zainstalowany serwer DNS, ponieważ takowego w domenie jeszcze nie ma, a jest niezbędny do jej prawidłowego funkcjonowania. Konieczne jest także podanie w kreatorze hasła niezbędnego w razie potrzeby przywracania usługi katalogowej.



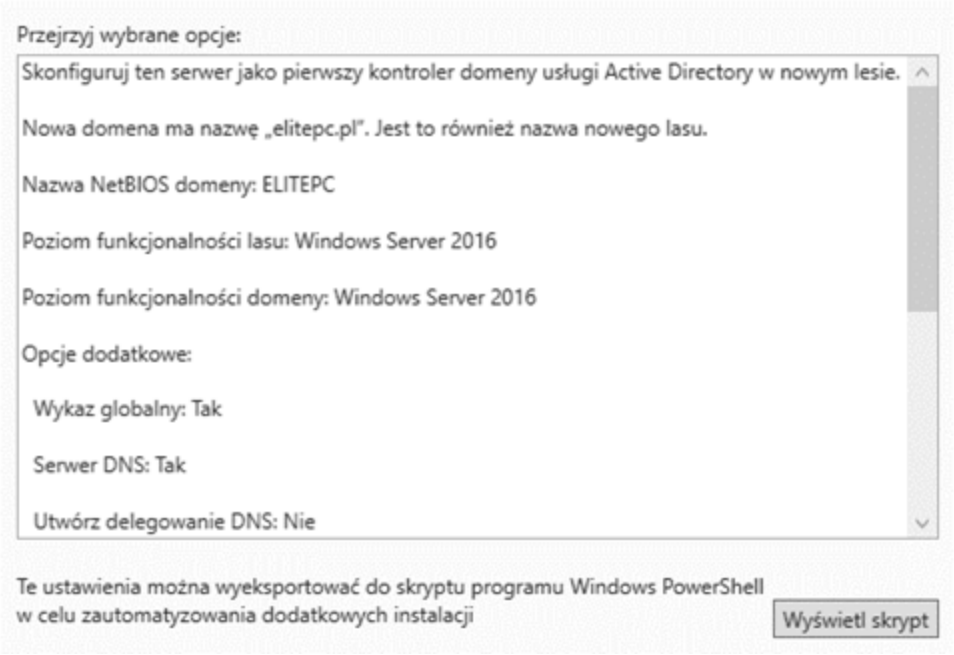
W następnej kolejności należy wybrać Dalej (Next).



Na kolejnej planszy nie są konieczne żadne zmiany, dlatego też należy przejść do następnej karty, klikając w Dalej (Next), chyba że nazwa kontrolera dla komputerów korzystających z NetBIOS ma być inna niż domyślna.

Podobnie jest w przypadku ścieżek, chyba że dane mają być przechowywane na osobnym nośniku.

Na planszy podsumowującej należy kliknąć w Dalej (Next).



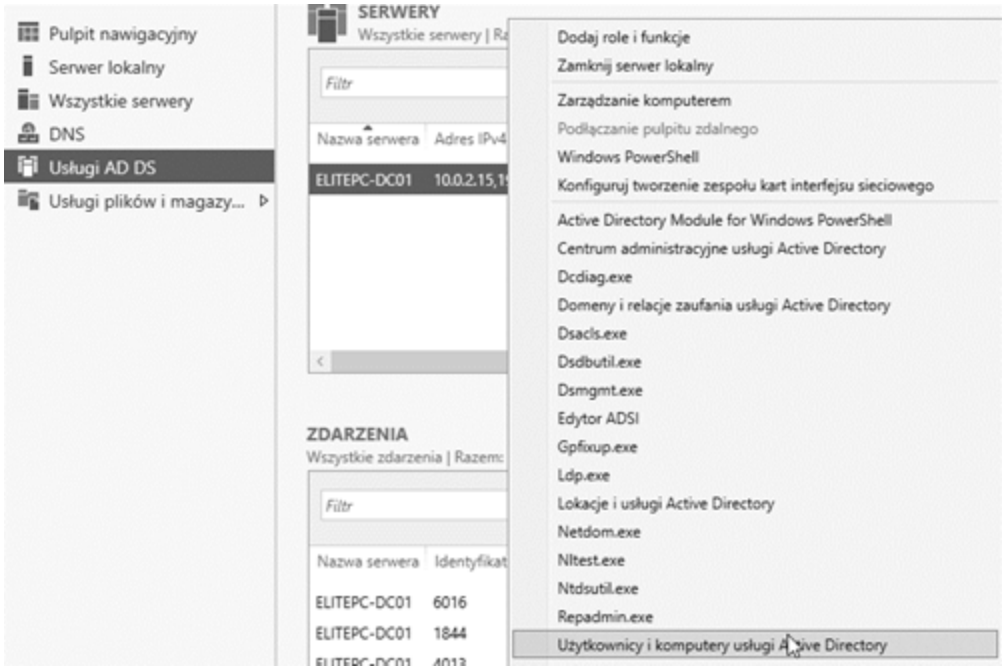
System zostanie poddany analizie. Jeżeli wszystko przebiegnie pomyślnie, można kliknąć w przycisk Zainstaluj (Install).

Proces instalacji zajmie dłuższą chwilę, należy zatem uzbroić się w cierpliwość.

3.4. Active Directory Users and Computers

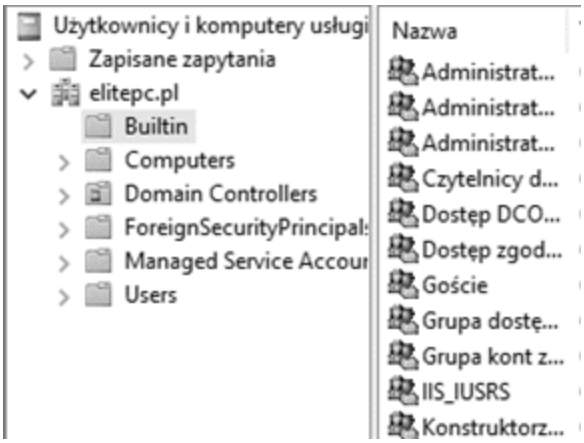
Po ponownym uruchomieniu komputera w Menadżerze Serwera (Server Manager) konieczne jest wybranie AD DS (Active Directory Domain Services), następnie na serwerze należy kliknąć prawym klawiszem myszy i wybrać

Komputery i Użytkownicy Usługi Active Directory (Active Directory Users and Computers).

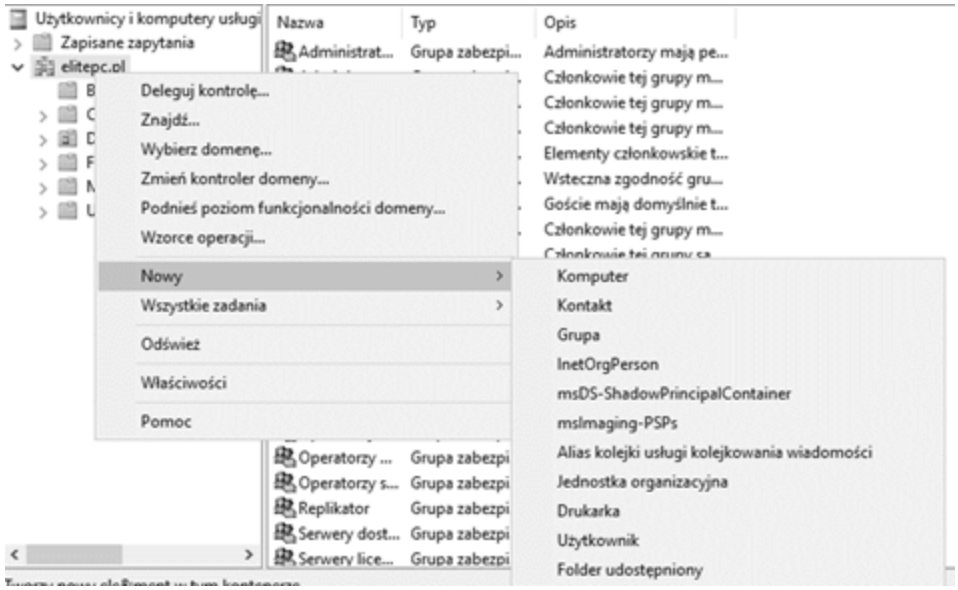


Jest to miejsce niezwykle ważnie, ponieważ będą w nim tworzone grupy i konta dla użytkowników oraz komputerów, będą im przypisywane odpowiednie role i uprawnienia. W system Windows jest już wbudowana całkiem pokaźna liczba grup bezpieczeństwa. W przykładzie nie będzie jednak potrzeby tworzenia nowych grup, mimo że daje to ogromne możliwości w przydzielaniu i odbieraniu uprawnień użytkownikom. Opis ról dostępny jest pod adresem:

http://technet.microsoft.com/pl-pl/library/cc756898%28WS.10%29.aspx .

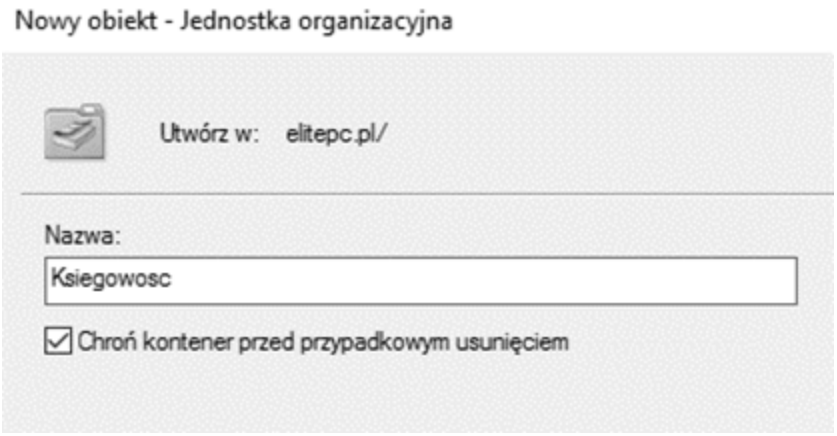


Przechodząc do praktyki, warto od samego początku utrzymywać ład i porządek, a także intuicyjne nazwy. Dlatego też na początku zostanie stworzona nowa Jednostka Organizacyjna. Dla zobrazowania, czym ona jest, można ją traktować jako byt podobny do katalogu. W celu jej utworzenia konieczne jest kliknięcie prawym klawiszem myszy na nazwie domeny, następnie w przycisk Nowy (New) i wybranie opcji Jednostka Organizacyjna (Organizational Unit).

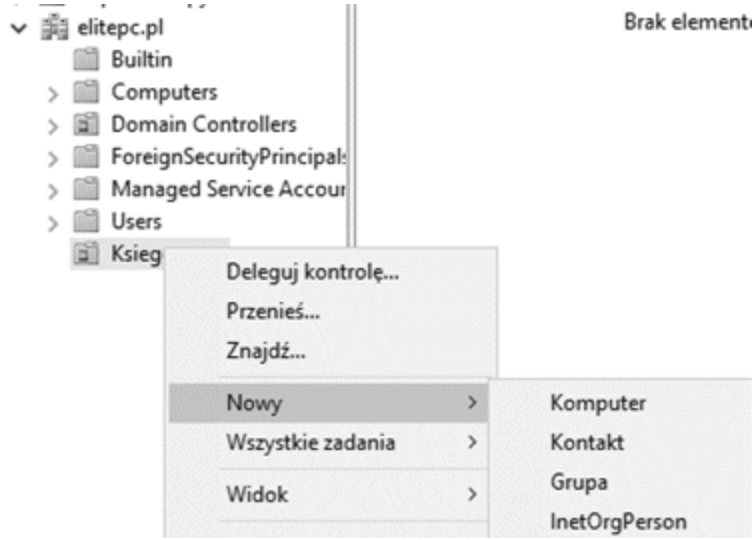


W ramach ćwiczenia zostanie stworzona jednostka organizacyjna o nazwie Księgowość (oczywiście, starając się

nie używać przy tym polskich znaków), gdzie będą przechowywani zatrudnieni księgowi. Wybór, a także akceptacja jej utworzenia zostaną zatwierdzone przyciskiem OK.

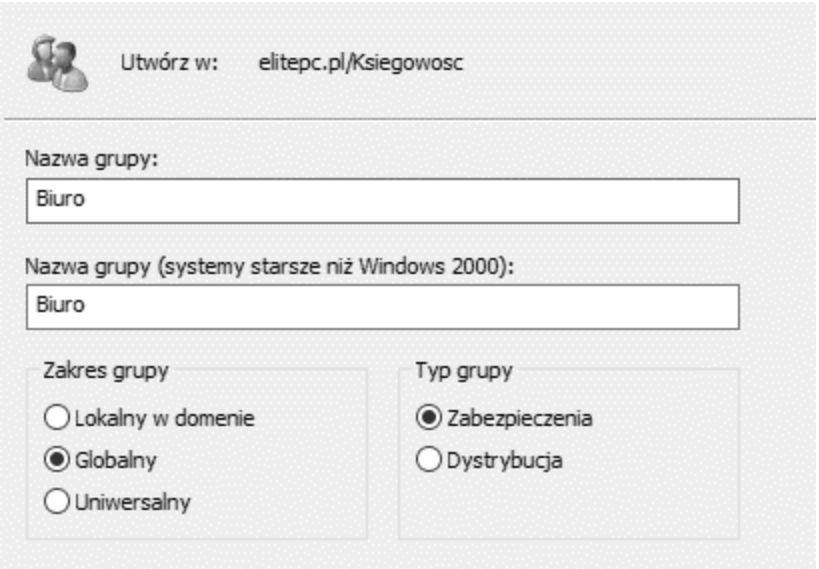


Następnie powstanie nowa grupa. W tym celu należy kliknąć prawym przyciskiem myszy na nowo powstałym elemencie, a następnie w Nowy (New) i Grupa (Group).



Dokonany zostanie podział na pracowników, którzy pracują na kasach oraz na tych, którzy pracują w biurze. Odpowiednio niech będą to grupy Kasa i Biuro. Czynność trzeba powtórzyć dla każdej z grup. Na planszy, która się pojawi, należy podać nazwę dla grupy oraz zaznaczyć opcje

w taki sam sposób, jak jest to zrobione na poniższej ilustracji i kliknąć przycisk OK.



Grupy dystrybucyjne mogą być używane tylko z aplikacjami poczty e-mail (np. Exchange) do wysyłania poczty e-mail do grup użytkowników. Grupy dystrybucyjne nie obsługują zabezpieczeń, co oznacza, że nie są wyświetlane na listach arbitralnej kontroli dostępu (DACL, Discretionary Access Control List). Jeśli jest potrzebna grupa służąca do kontroli dostępu do zasobów udostępnionych, należy utworzyć grupę zabezpieczeń.

Grupy zabezpieczeń, jeśli są używane z rozwagą, stanowią wydajny sposób udzielania dostępu do zasobów w sieci.

Za pomocą grup zabezpieczeń można wykonywać następujące operacje:

- Przypisywanie praw użytkownika grupom zabezpieczeń w usłudze Active Directory. Prawa użytkownika są przypisywane grupie zabezpieczeń w celu ustalenia

czynności, jakie członkowie danej grupy mogą wykonać w zakresie domeny (lub lasu). Prawa użytkownika są automatycznie przypisywane niektórym grupom zabezpieczeń podczas instalowania usługi Active Directory, aby ułatwić administratorom określenie roli administracyjnej poszczególnych osób w domenie. Na przykład użytkownik dodany do grupy „Operatorzy kopii zapasowych” w usłudze Active Directory może wykonywać kopie zapasowe plików i katalogów znajdujących się na każdym kontrolerze domeny, a także przywracać te pliki i katalogi z kopii zapasowych. Jest to możliwe, ponieważ domyślnie grupie „Operatorzy kopii zapasowych” są automatycznie przypisywane prawa użytkownika, wykonywanie kopii zapasowych plików i katalogów oraz przywracanie plików i katalogów, a członkowie grupy dziedziczą prawa użytkownika przypisane grupie.

- Za pomocą przystawki Zasady grupy (Group Policies) można przypisać grupom zabezpieczeń prawa użytkownika, aby ułatwić delegowanie określonych zadań. Przypisując delegowane zadania, należy zachować dużą ostrożność, ponieważ niedoświadczony użytkownik mający zbyt wiele praw w grupie zabezpieczeń stanowi zagrożenie dla bezpieczeństwa sieci.

- Przypisywanie uprawnień do zasobów grupom zabezpieczeń. Uprawnień nie wolno mylić z prawami użytkownika. Uprawnienia przypisuje się grupom zabezpieczeń dla danego zasobu udostępnionego. Decydują one o tym, kto ma mieć możliwość dostępu do zasobu i na

jakim poziomie, np. pełna kontrola (Full Control). Niektóre uprawnienia są przypisywane automatycznie, np. dla obiektów domeny, po to, aby określić różne poziomy dostępu domyślnych grup, jak np. Administratorzy domeny czy Operatorzy kont.

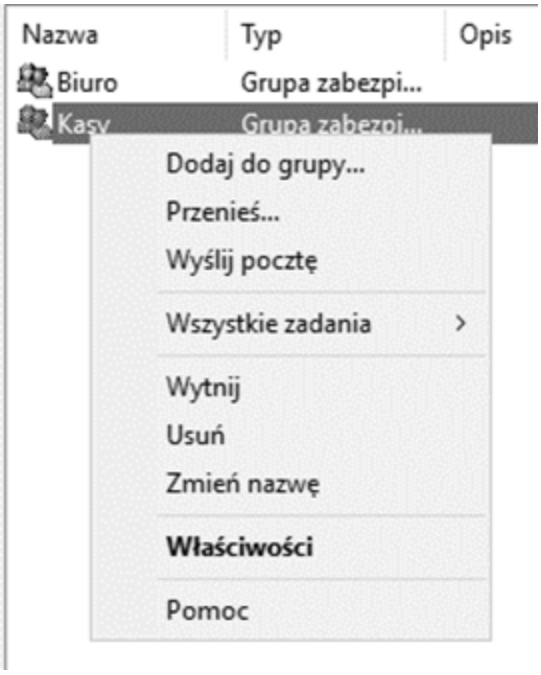
Grupy zabezpieczeń wymieniane są na listach DACL. Listy te określają uprawnienia do obiektów i zasobów. Administratorzy powinni przypisywać uprawnienia do zasobów (drukarek, udziałów plików itp.) nie pojedynczym użytkownikom, lecz całym grupom zabezpieczeń. Przypisywanie uprawnień grupie jest o tyle wygodne, że nie trzeba powtarzać wielokrotnie tej samej procedury. Każde konto, które zostało przydzielone do grupy, otrzymuje prawa narzucone tej grupie w usłudze Active Directory, tak samo jak i uprawnienia tej grupy do określonych zasobów.

Grupy zabezpieczeń, podobnie jak grupy dystrybucyjne, mogą zostać użyte jako adresaci poczty e-mail. Gdy zostanie wysłana wiadomość e-mail do danej grupy, otrzymają ją wszyscy jej członkowie.

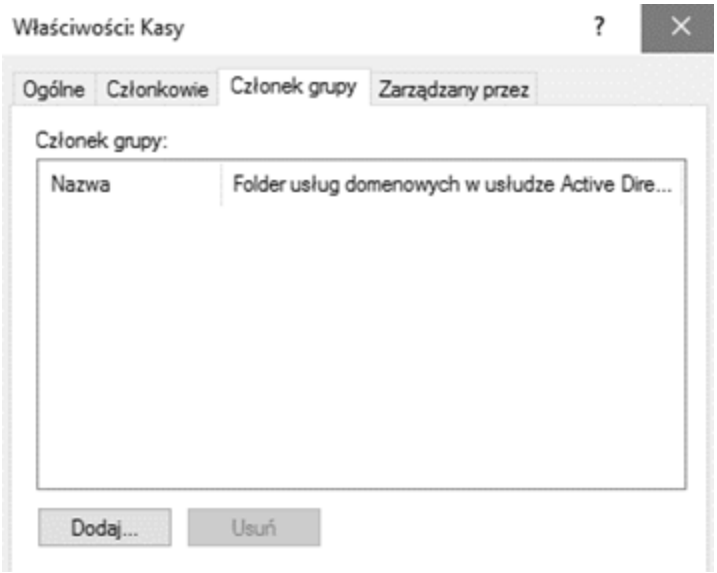
Grupy będą bardzo pomocne, jeśli większej liczbie użytkowników zostaną przypisane dane uprawnienia, a innej już nie, np. w ćwiczeniowym przypadku kasjerzy nie powinni mieć tak wysokich uprawnień jak pracownicy biurowi.

Naturalnie, tak utworzonej grupie należałoby nadać odpowiednie prawa. Na przykład niech to będą prawa zwykłego Użytkownika. Zostanie więc wykorzystana wbudowana w system Windows grupa bezpieczeństwa.

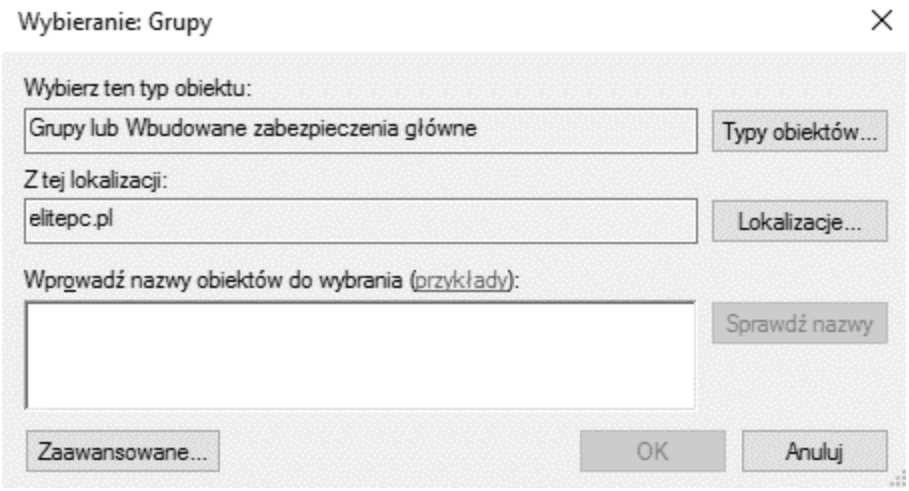
W tym celu należy kliknąć prawym klawiszem myszy na Właściwości (Properties) np. kasjerów.



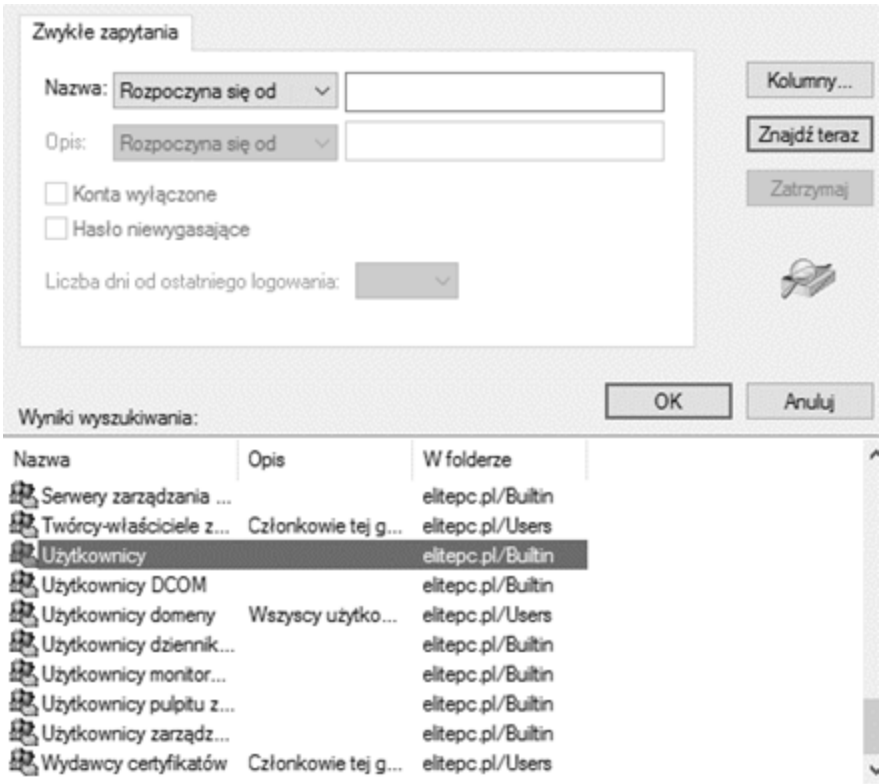
W oknie, które się pojawi, konieczne jest przejście do zakładki Członek Grupy (Member Of) i wybranie przycisku Dodaj (Add).



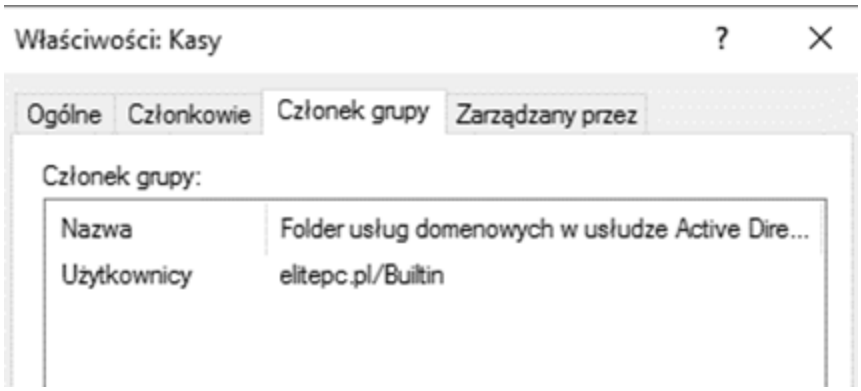
Następnie należy kliknąć w Zaawansowane (Advanced).



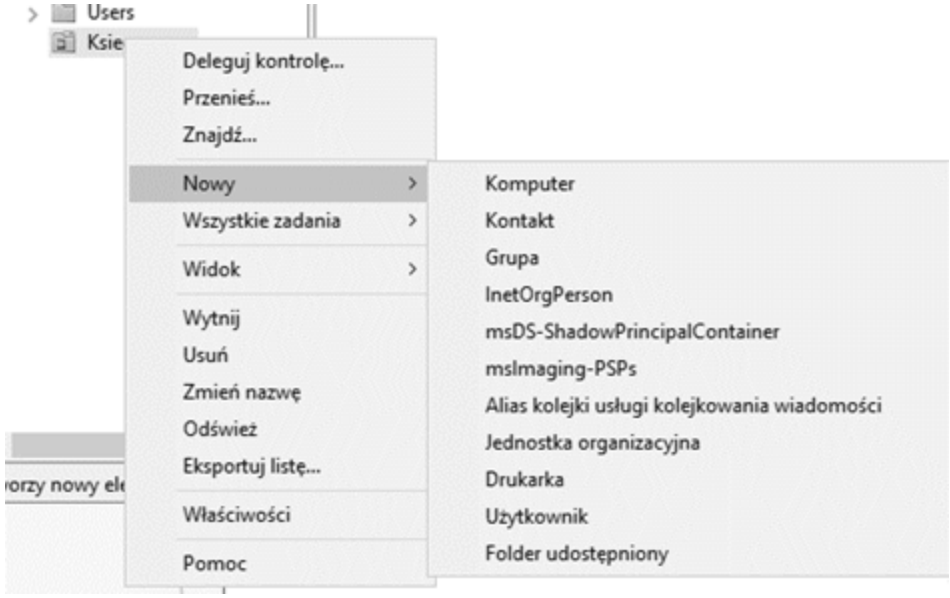
W dalszej kolejności należy kliknąć w Znajdź teraz (Find Now), a z listy, jaka się wygeneruje, wybrać Użytkownicy (Users) i kliknąć w przycisk OK, a następnie jeszcze raz OK.



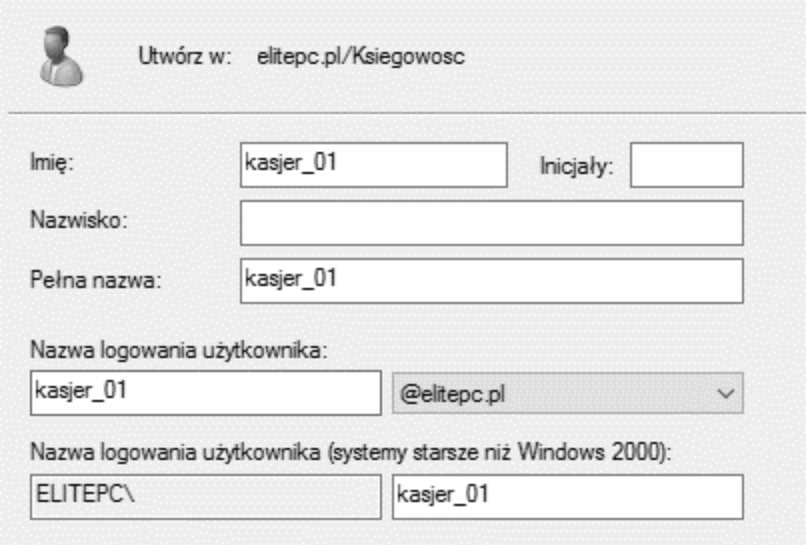
Jak widać, kasjerzy są już w Użytkownikach. Należy kliknąć w OK.



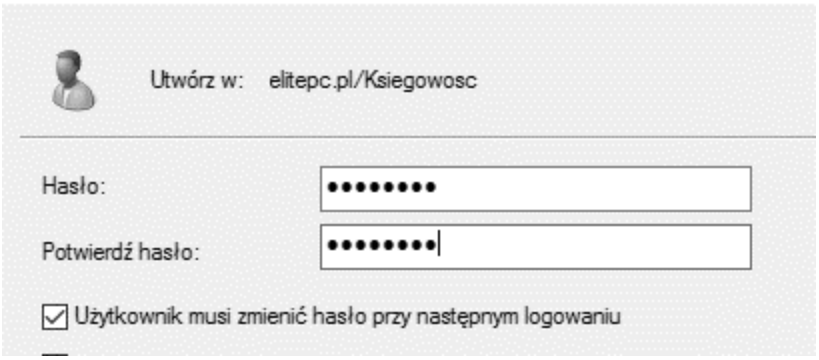
Dla testu zostanie dodany użytkownik, na którym będą przeprowadzane różne doświadczenia w dalszej części książki. W celu stworzenia użytkownika należy prawym przyciskiem myszy kliknąć w Księgowość > Nowy (New) > Użytkownik (User).



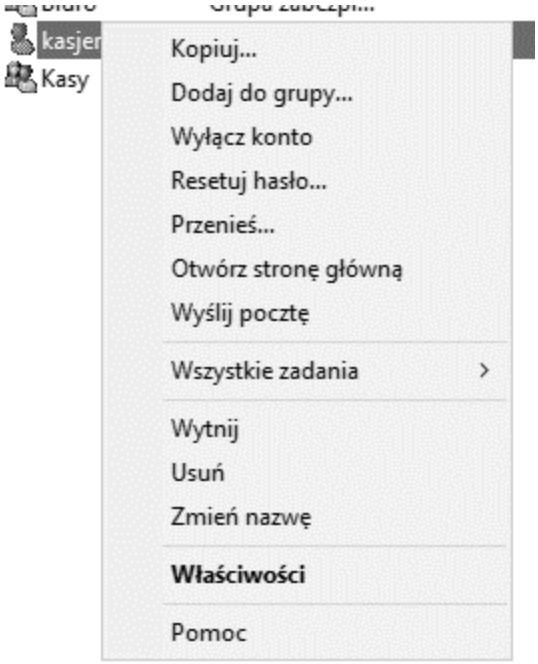
Trzeba wypełnić wszystkie pola. Ważna jest nazwa logowania użytkownika, gdyż to dzięki niej będzie się on mógł zalogować na danym komputerze. W przykładzie zastosowano nazwę kasjer_01.



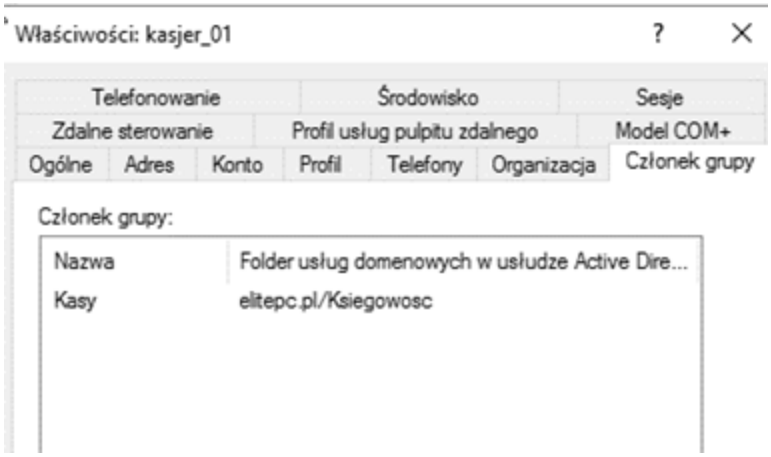
Na następnej karcie należy wybrać dla tego użytkownika odpowiednie hasło. Warto zostawić zaznaczoną opcję Użytkownik musi zmienić hasło przy następnym logowaniu (User must change password at next logon), aby mógł sobie w trakcie pierwszego logowania je zmienić wedle własnych upodobań. Potem należy kliknąć w Dalej (Next), a następnie Zakończ (Finish).



W następnej kolejności należy wejść w jego Właściwości (Properties), klikając prawym przyciskiem myszy, a następnie w zakładkę Członek Grupy (Member of).



Domyślnie jest on Użytkownikiem Domeny (Domain Users). Można więc skasować tą pozycję, a potem dodać go do grupy „Kasy”.

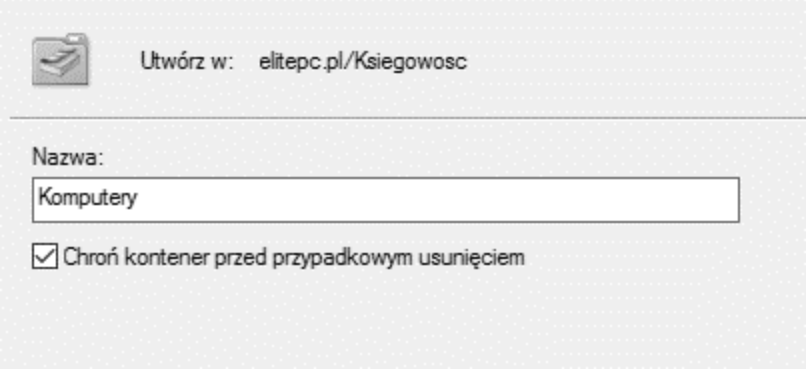


Grupę Kasy można natomiast teraz przypisać do grupy Użytkownicy Domeny (Domain Users). To, co zostało uzyskane, to pewnego rodzaju hierarchia (dziedziczenie). Użytkownicy należą do grupy Kasy, a grupa Kasy należy do jednej lub więcej innych grup. Dzięki temu można

swobodnie zarządzać uprawnieniami wielu użytkowników naraz, zamiast każdego użytkownika z osobna.

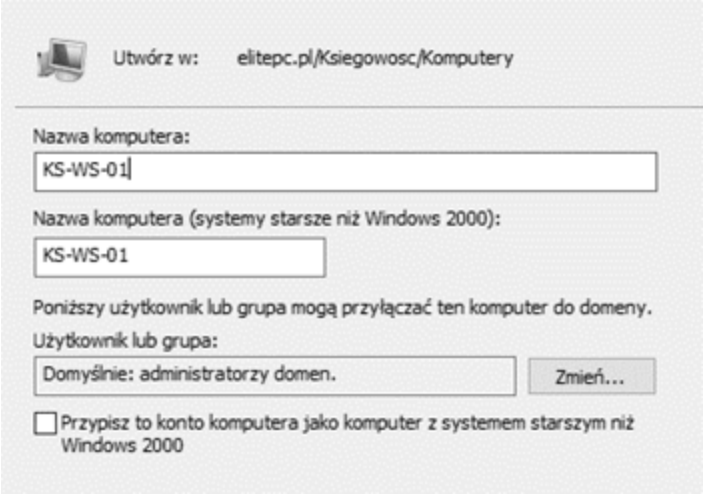
Należy sprytnie zarządzać zarówno grupami użytkowników jak i jednostkami organizacyjnymi, ponieważ nie tylko ułatwi to pracę administratorowi systemu i zwiększy bezpieczeństwo, ale także pozwoli wydajnie zarządzać, np. Zasadami grupy, które można przyłączać wyłącznie do jednostek organizacyjnych.

Zostanie teraz stworzona kolejna jednostka organizacyjna, lecz tym razem wewnątrz księgowości. Zostanie nazwana „Komputery”. Będą tam przechowywane konta dla komputerów w tym dziale.

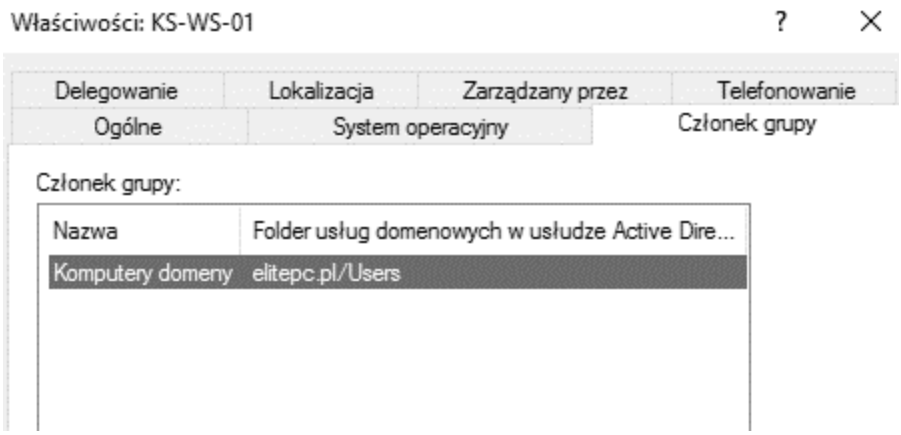


Teraz należy kliknąć prawym przyciskiem myszy na Komputery > Nowy > Komputer (Komputery > New > Computer).

Następnie należy stworzyć maszynę, która będzie się nazywać „KS-WS-01”.

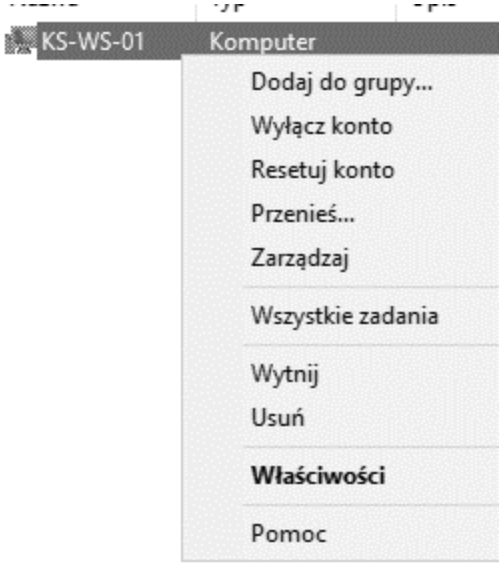


Komputer domyślnie zostanie przypisany do grupy Komputery Domeny (Domain Computers). Co można sprawdzić, klikając w jego Właściwości (Properties).

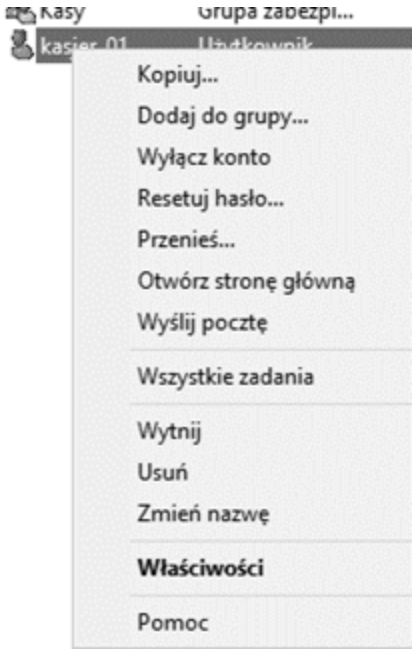


Trzeba pamiętać, że każdy komputer z systemem Windows NT, Windows 2000 lub nowszym, który zostaje dołączony do domeny, otrzymuje własne konto komputera. Podobnie jak konta użytkowników, konta komputerów umożliwiają uwierzytelnianie oraz inspekcję dostępu komputera do sieci i zasobów domeny. Każde konto komputera musi być unikatowe. Uniemożliwi to niepowołanym osobom podłączenie się do sieci bez zgody administratora. Skoro zostali już stworzeni i pogrupowani

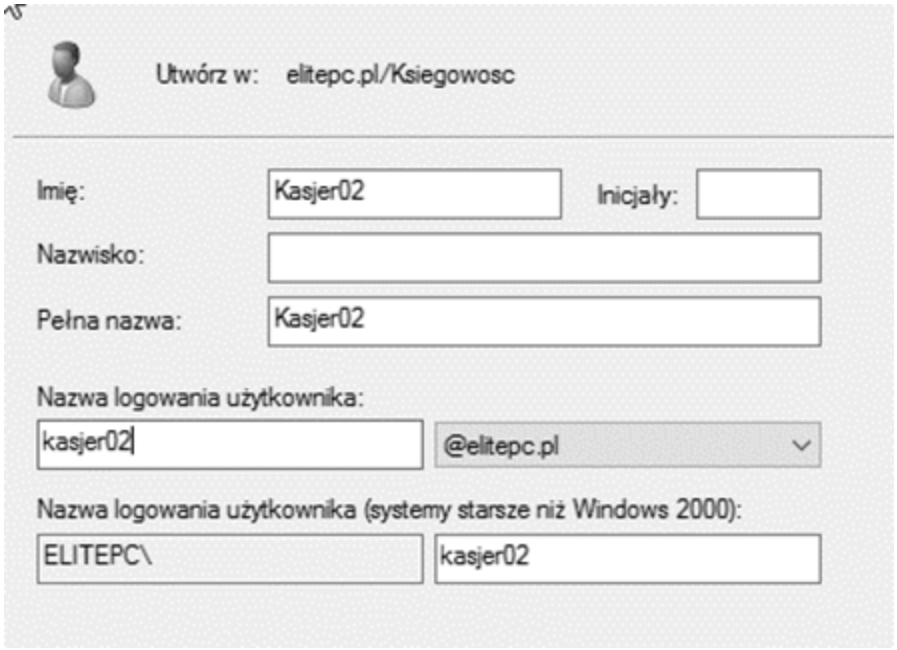
użytkownicy oraz konta komputerów, warto jeszcze zwrócić uwagę na ich właściwości. Po kliknięciu prawym przyciskiem myszy na koncie komputera są dwie ważne opcje. Jedną z nich jest Wyłączenie Konta (Disable Account), a drugą Zresetowanie Konta (Reset Account). Ta druga niezbędna jest wtedy, gdy maszyna o danej nazwie uległa awarii i została wymieniona na nową. Nowego komputera nie podłączy się do domeny do chwili zresetowania konta.



W przypadku konta użytkownika również można je wyłączyć, a także zresetować mu hasło opcją Resetuj Hasło (Reset Password). Przydatna jest także możliwość Wysłania Wiadomości (Send Mail).



Kont użytkownika z założenia nie powinno się kasować z kilku względów. Jednym z nich jest to, że na miejsce danego pracownika może przyjść jego następca – musiałoby wtedy zostać utworzone dla niego nowe konto, wprowadzone wszelkie ustawienia oraz uprawnienia. Prościej będzie użyć opcji Kopiuj (Copy).

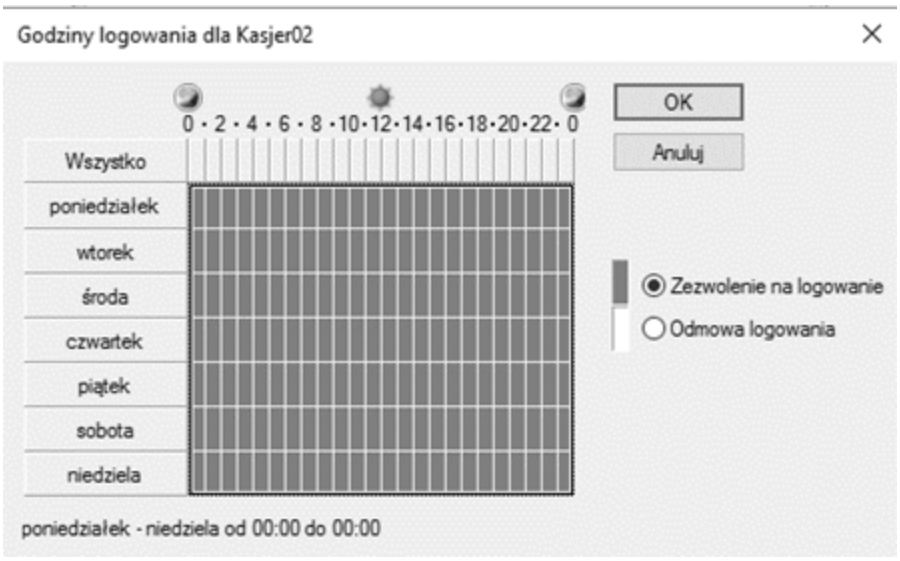


Będzie konieczne podanie nowej nazwy użytkownika oraz hasła, natomiast wszelkie inne ustawienia, jak np. uprawnienia czy zamontowane dyski sieciowe, pozostaną zachowane. Z racji tego, że na ogół ustawień jest dość dużo, praktykuje się właśnie stworzenie wzorcowego konta użytkownika w obrębie danej Grupy i kopiowanie, zamiast tworzenia za każdym razem nowego konta. Użytkowników, którzy przestają być potrzebni, najlepiej wyłączyć i przenieść do wcześniej przygotowanej jednostki organizacyjnej (np. czasowo wyłączeni). Można teraz wejść we właściwości jakiegoś konta użytkownika.

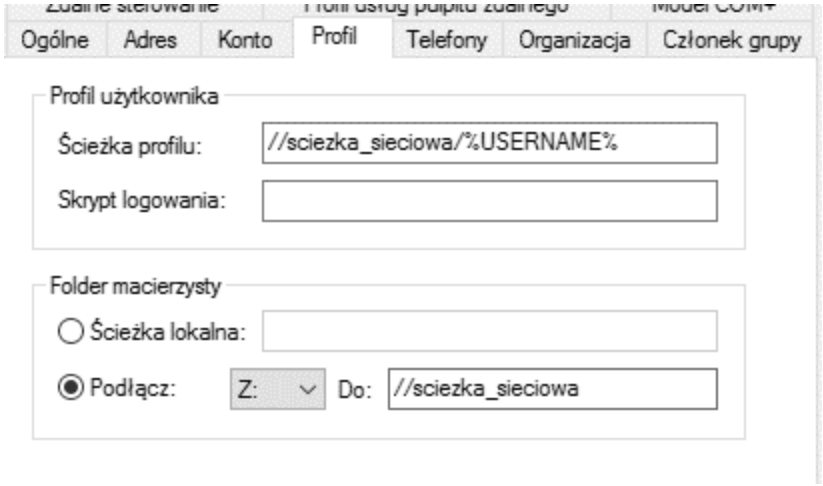
W zakładkach Ogólne (General), Adres (Address), Telefony (Telephones) i Organizacja (Organization) znajdują się jedynie pola, w których można wpisać jakieś informacje o użytkowniku.

W zakładce Konto (Account) warto zwrócić uwagę na to, iż można zmienić login użytkownika lub nadać inny dla różnych domen. Warto korzystać z funkcji Wygasania ważności konta (Account Expires), która powoduje wyłączenie konta po upływie daty jakiegoś czasu (np. w dniu końca umowy o pracę). Dzięki temu administrator nie musi pamiętać o wyłączeniu konta zwolnionego pracownika.

Bezpieczeństwo sieci można dodatkowo zwiększyć za pomocą ustawień Godzin Logowania (Logon Hours).

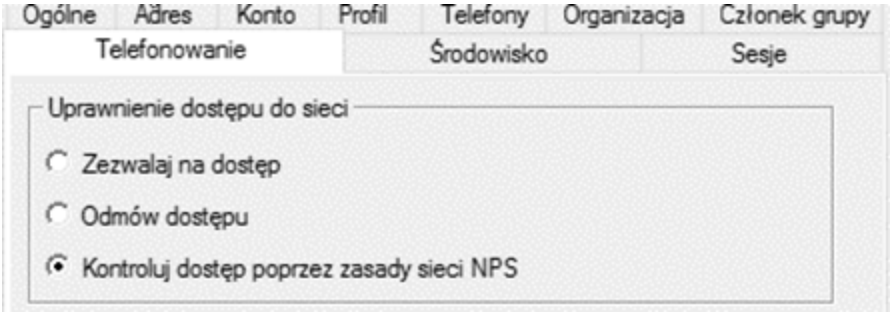


Łatwym sposobem można określić to, w jakich godzinach konto może być używane, a w jakich nie. Dzięki temu potencjalny włamywacz, jeżeli nawet dostanie się na takie konto, poza godzinami pracy, czyli wtedy, gdy nie ma nadzoru nad siecią, nie będzie w stanie niczego zrobić.

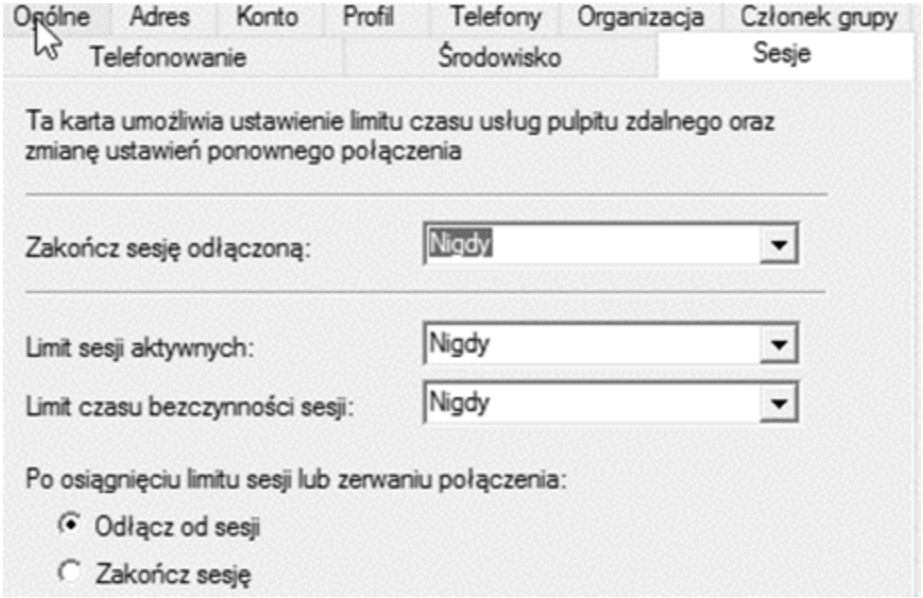


W zakładce Profil (Profile) można określić ścieżkę sieciową dla profilu, czyli lokalizację w sieci, gdzie dany profil ma być przechowywany. Parametr %USERNAME% to zmienna środowiskowa, która zwraca nazwę użytkownika. Dzięki temu w podanej lokalizacji zostanie utworzony katalog o nazwie takiej samej, jak nazwa użytkownika. Kopiując tak

skonfigurowany profil, pewne jest, że każdy nowy użytkownik dostanie swój własny prywatny folder w zasobie sieciowym. Istnieje także możliwość zamontowania dysku sieciowego. Niestety ograniczona do jednego dysku. Więcej można zamontować za pomocą Zasad Grupy.



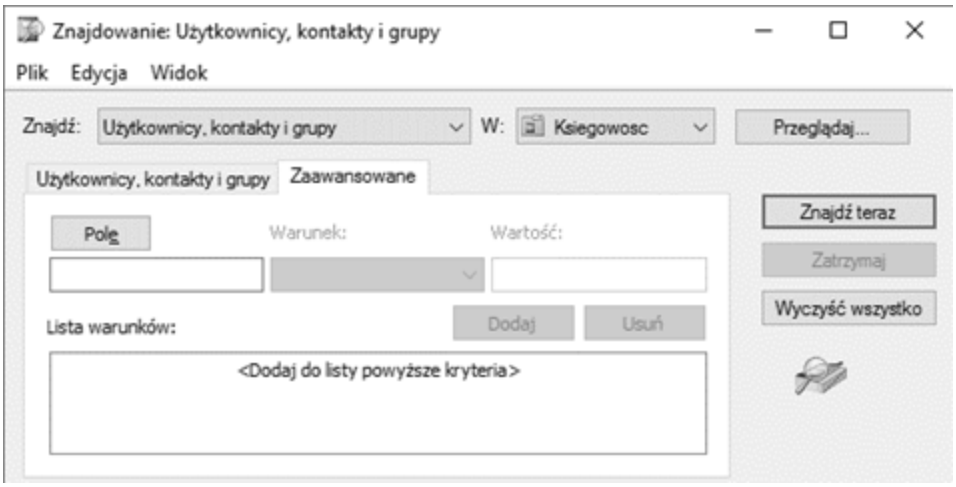
W zakładce Telefonowanie (Dial –in) warto zwrócić uwagę na to, czy użytkownik ma zgodę na dostęp do sieci z zewnątrz. Jeżeli takiej nie ma, to np. nie będzie mógł się podłączyć do wewnętrznej sieci za pomocą VPN'a itp. Na taki dostęp można mu pozwolić lub wybrać opcję trzecią, która mówi o tym, że NPS zajmie się jego weryfikacją (o czym już w dalszych działach).



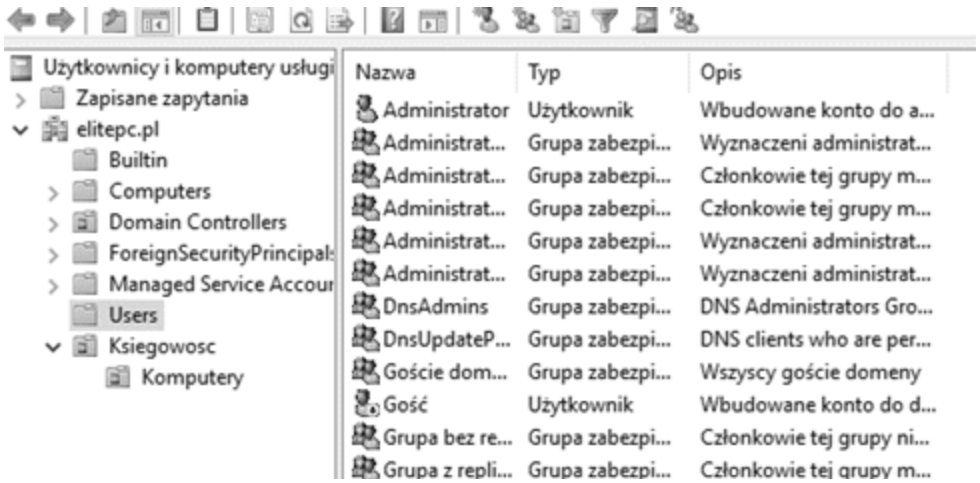
Ze względów licencyjnych, i nie tylko, w zakładce Sesje (Sessions) warto ustawić limity czasu trwania sesji tak, aby użytkownicy nieaktywni lub tacy, którzy zostawili włączone komputery przed wyjściem z pracy, byli automatycznie wylogowywani.

Za pomocą ikonki

można dostać się do wyszukiwarki Active Directory, w której można tworzyć kwerendy, przefiltrowujące dokładnie całą usługę katalogową i pomagające wyłuskać pożądane informacje.



Zamykając dział dotyczący Active Directory, warto nadmienić, iż ze względów wydajnościowych w obrębie jednostki organizacyjnej nie powinno znajdować się więcej niż 5000 użytkowników.

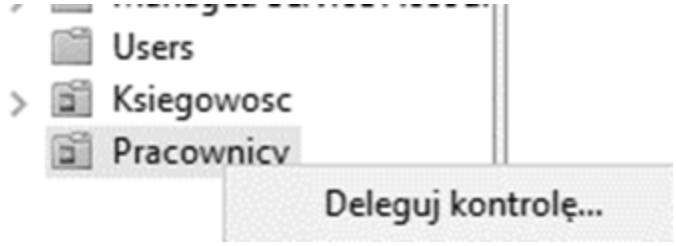


Warto także pamiętać, że w jednostce organizacyjnej Użytkownicy (Users) znajduje się bardzo newralgiczne konto Administrator.

Każdy użytkownik Windows posiada Identyfikator Bezpieczeństwa (Security Identifier), który wygląda mniej więcej tak: S-1-5-21-3627861015-3361044348-30300820-1013. Konto Administrator posiada na samym końcu zawsze liczbę 500, czyli wygląda mniej więcej tak: S-1-5-21-3623811015-3361897348-30300820-500. Dzięki temu potencjalny włamywacz posiada wiedzę na temat tego, które konto to Administrator. Dlatego też jednym z pierwszych kroków w pracy z Active Directory powinno być powielenie konta administratora. Można to osiągnąć wyłącznie poprzez opcję Kopiuj (Copy), a następnie wyłączenie pierwotnego konta z wcześniejszym nadaniem mu bardzo złożonego hasła.

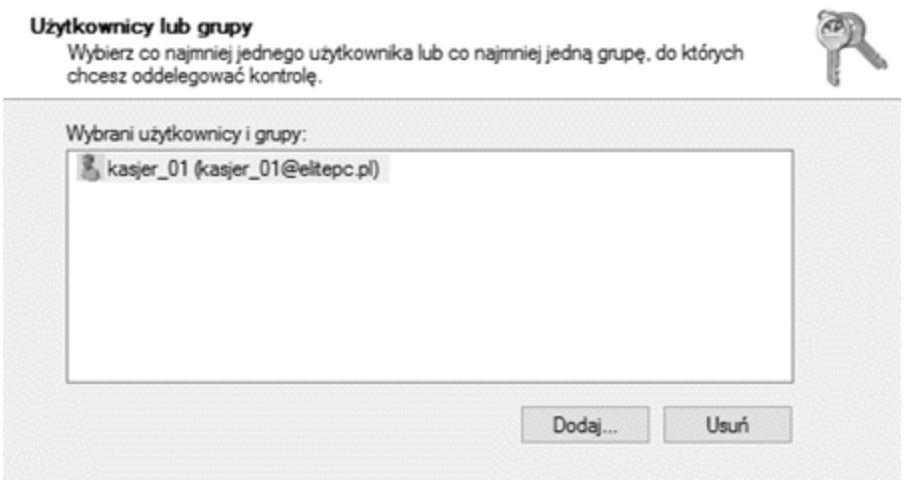
Naturalnie administrator nie jest osobą odpowiedzialną za całe działanie serwera. Na ogół różne osoby zarządzają różnymi rolami, a nawet częściami ról. Tak samo jest w przypadku Active Directory. W celu przeprowadzenia

demonstracji, należy stworzyć jednostkę organizacyjną Pracownicy oraz użytkownika Szef. Następnie na jednostce organizacyjnej Pracownicy należy przycisnąć prawy przycisk myszki i wybrać Deleguj kontrolę (Delegate Control).

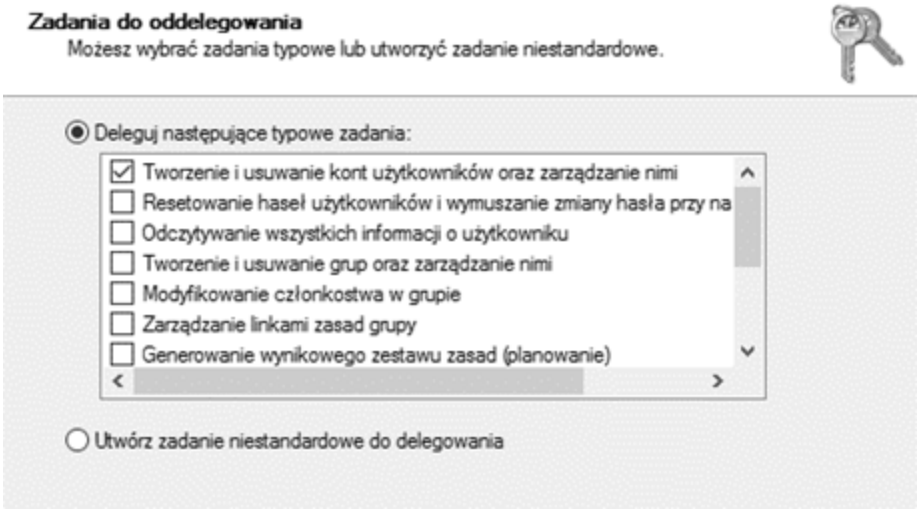


Ukaże się kreator, który pozwala na przedelegowanie kontroli nad pojedynczą jednostką organizacyjną i jej zawartością wybranemu użytkownikowi. Użytkownik ten będzie mógł zarządzać innymi użytkownikami, nadawać im uprawnienia, tworzyć grupy, komputery, jednostki organizacyjne oraz inne obiekty Active Directory, lecz tylko wewnątrz jednostki organizacyjnej Pracownicy. Należy kliknąć Dalej (Next).

Kolejne okno kreatora służy do określenia tego, komu kontrola zostanie przedelegowana. Tych użytkowników lub ich grupy dodaje się przyciskiem Dodaj (Add).



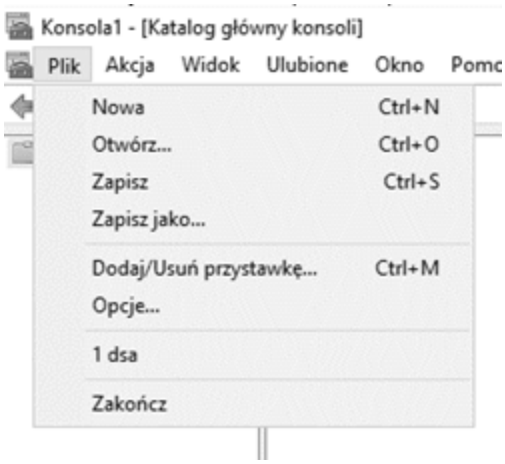
Następnie należy określić, jakie zadania dany użytkownik będzie mógł realizować. Do wyboru jest kilka predefiniowanych szablonów. Istnieje także możliwość stworzenia nieszablonowego zadania.



Na karcie podsumowującej należy kliknąć Zakończ (Finish).

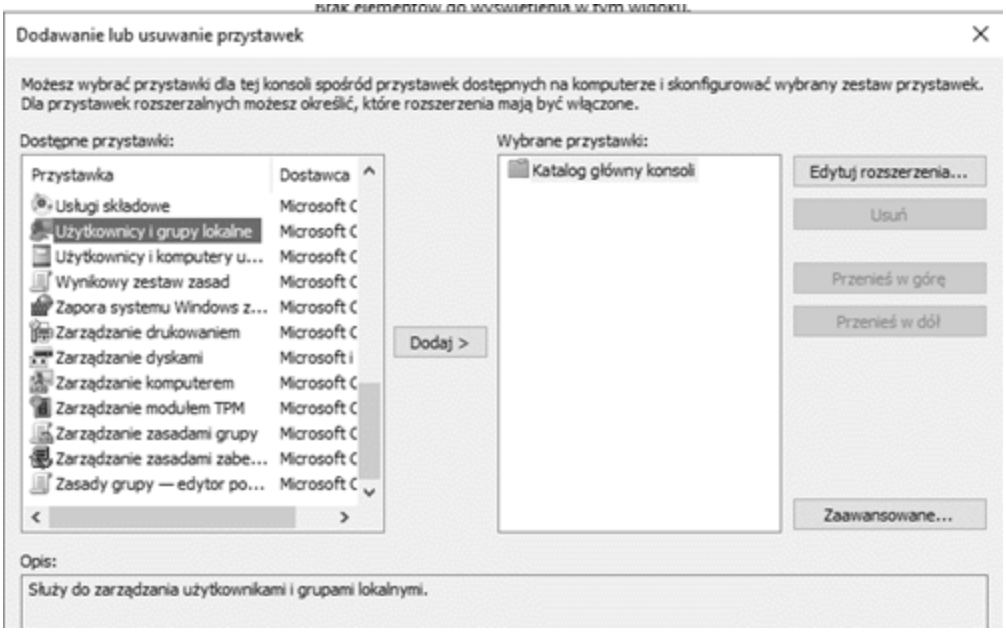
Fizyczny dostęp do serwera jest niewskazany nawet dla administratora, a tym bardziej dla zwykłego użytkownika. Dlatego też należy dać użytkownikom możliwość zarządzania rolami, do których mają dostęp. Można to uczynić, tworząc własną konsolę MMC. Aby ją stworzyć w menu Start należy wyszukać aplikację MMC i ją uruchomić.

W programie, który się uruchomi, należy wybrać Plik (File) i opcję Dodaj/Usuń Przystawkę (Add or Remove Snap-ins).

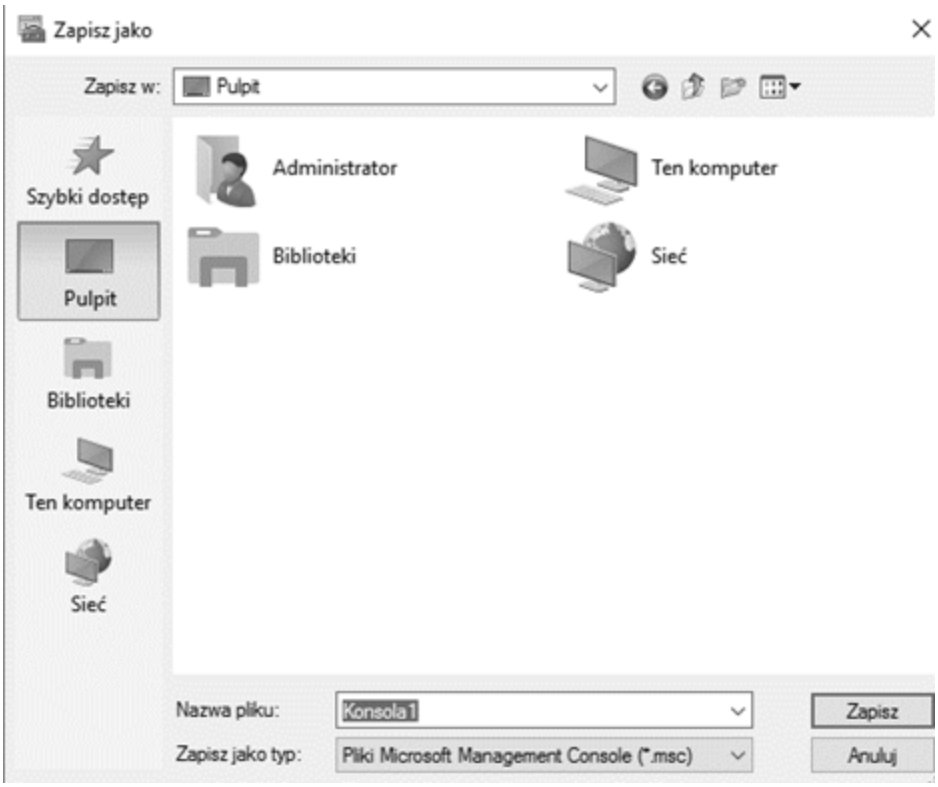


Pojawi się okno, w którym z listy po lewej stronie wybiera się, które konsole mają być dołączone do obecnie tworzonej

za pomocą guzika Dodaj (Add).



Tak przygotowaną konsolę należy zachować wybierając Plik (File), a następnie Zapisz (Save). Konsoli należy nadać przyjazną nazwę, tak aby odzwierciedlała to, co się w niej znajduje. Tym bardziej, że jej zawartość może składać się z kilku standardowych konsol, np. może zawierać przystawki do zarządzania DNS, DHCP czy Active Directory itp.



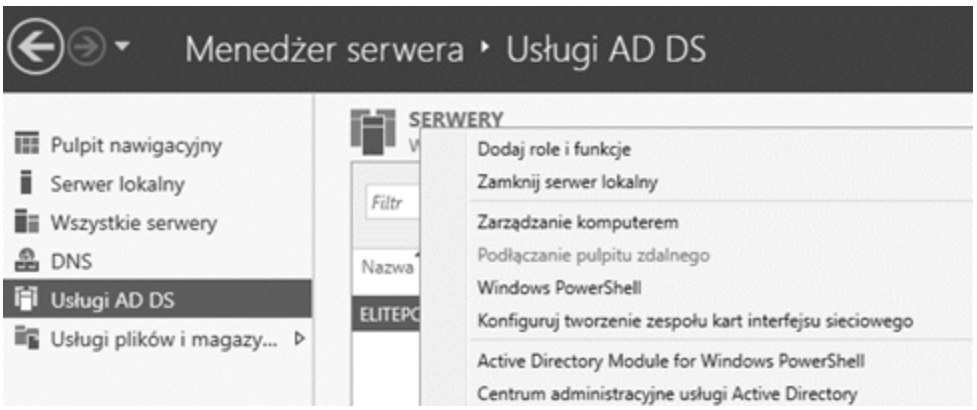
Tak przygotowany plik wystarczy przekazać użytkownikom docelowym. Musi on zostać uruchomiony na komputerze wpiętym do sieci firmowej bezpośrednio bądź przez VPN. Uruchomienie następuje poprzez dwukrotne kliknięcie na konsoli, a sposób zarządzania nie odbiega od tego bezpośrednio z serwera.

Inną opcją udzielenia komuś możliwości zarządzania np. nad pojedynczą grupą jest udzielenie władzy poprzez jej Właściwości (Properties) i wybranie zakładki Zarządzany przez (Managed by). Karta ta pozwala na przypisanie jednego użytkownika do zarządzania jedną konkretną grupą.

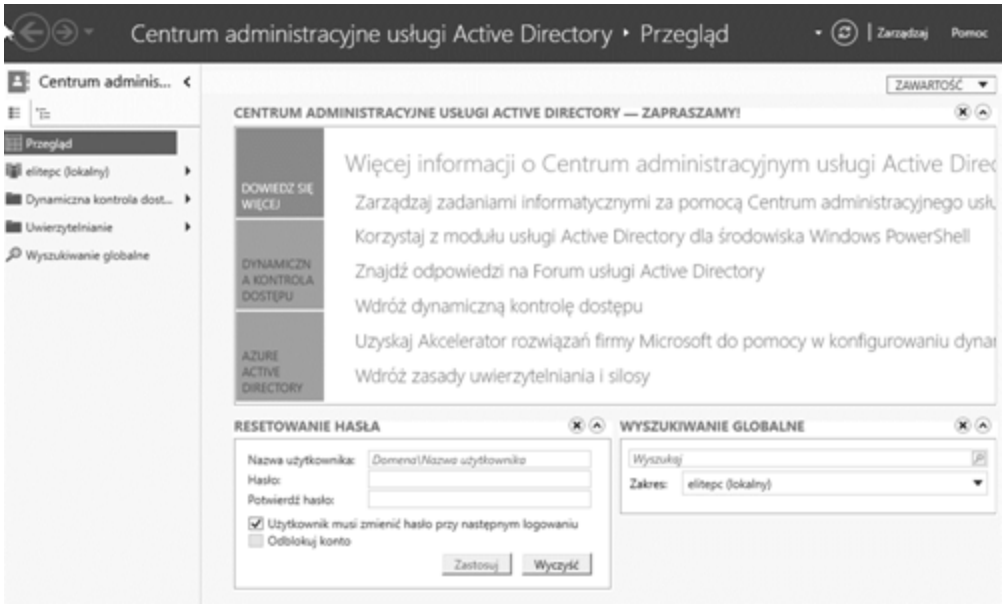
3.5. Active Directory Administrative Center

Chyba najlepszą i zarazem najbardziej popularną usługą katalogową jest Active Directory. Mimo że jest ona wciąż na bieżąco rozwijana, to jednak należy pamiętać, że wywodzi się jeszcze z czasów Windows 2000. Nic więc dziwnego, że Microsoft stara się ciągle nie tylko dopracowywać starą, ale także tworzyć być może lepsze rozwiązania, które będą w stanie zastąpić swoich poprzedników. Jedną z takich nowości jest przystawka Centrum Administracyjne Active Directory (Active Directory Administrative Center). Została ona wprowadzona w Windows Serwer 2008 R2, a w rozwiniętej wersji zaimplementowana również w Windows Server 2016.

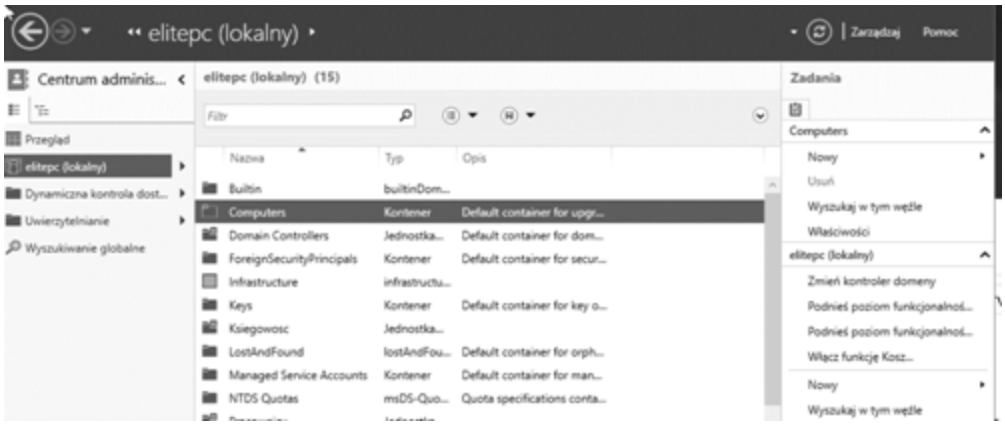
Choć na pierwszy rzut oka wygląda ona do złudzenia podobnie do tej z Windows Server 2008, to wprowadza kilka nowych możliwości. Podobnie jak inne konsolki, znajduje się ona w narzędziach administracyjnych. Można się do niej dostać także poprzez Menadżera Serwera, analogiczne do Użytkowników i Komputerów usługi Active Directory.



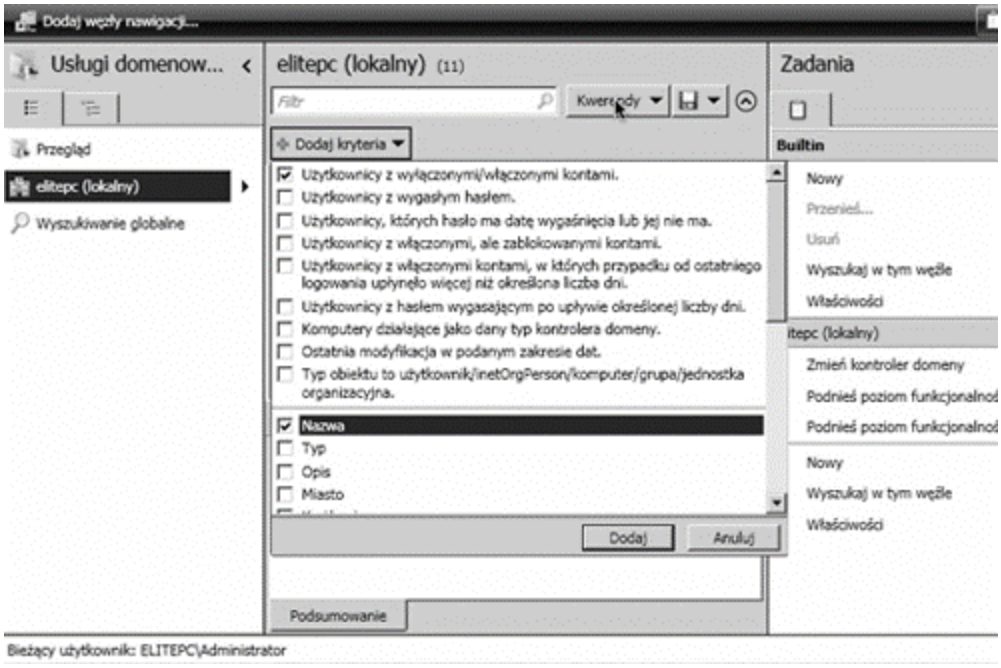
Celem jej wprowadzenia było uproszczenie, przyspieszenie i ułatwienie wykonywania najczęstszych czynności, jakie administrator napotyka na swojej drodze. Zostaną więc tutaj stworzeni użytkownicy, grupy, kontenery, jednostki administracyjne itp. Można przy tym jednocześnie zarządzać więcej niż jedną domeną, używać filtrów wyszukiwania oraz powiązać jej pracę z PowerShell'em. Już pierwsza karta pozwala na zresetowanie hasła użytkownika czy przeszukanie domeny.



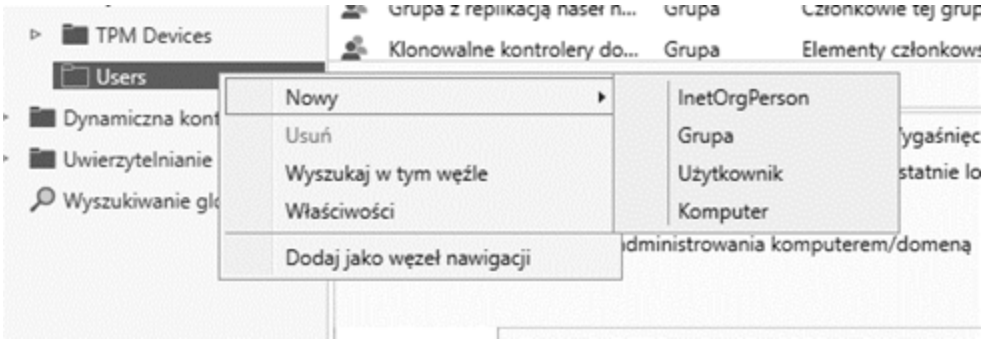
Po kliknięciu z lewej strony na pożądaną domenę, w środkowej części ekranu pojawi się pasek z możliwością ręcznego pisania kwerend oraz zawartością domeny. Na pierwszy rzut oka wygląda podobnie do starej przystawki.



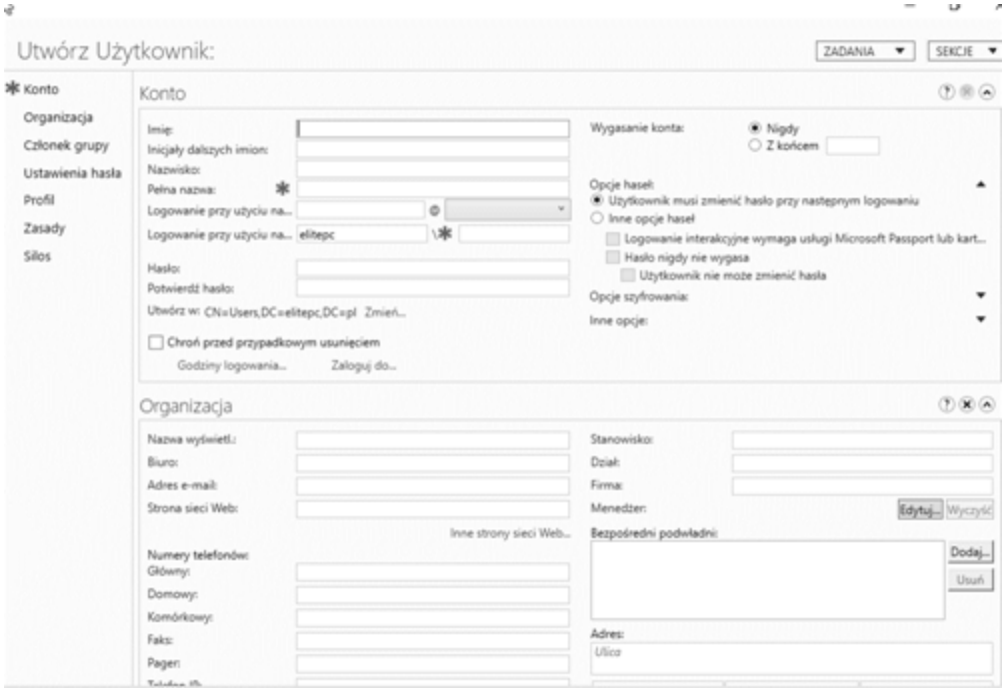
Klikając w Dodaj kryteria (Add Criteria) można wybrać interesujące administratora właściwości obiektów, według których będą filtrowane wartości.



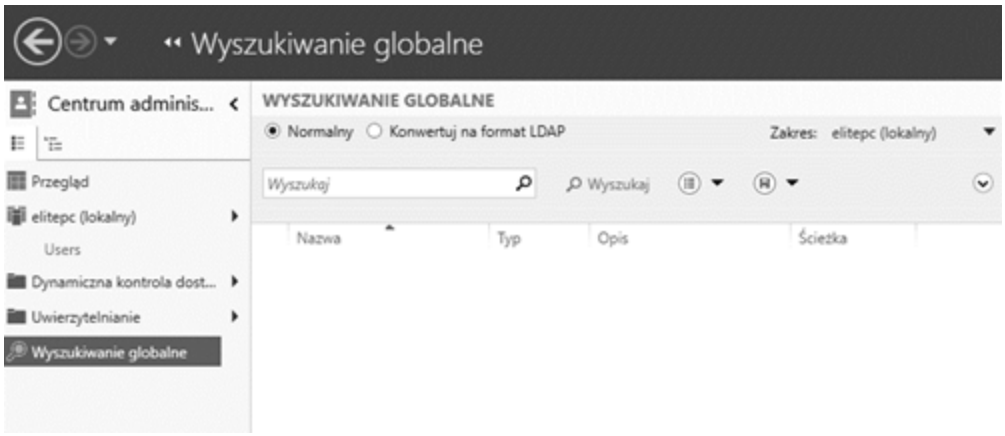
Ogólnie rzecz ujmując, zarządzanie jest bardzo podobne do przystawki Użytkownicy i komputery usługi Active Directory. Można np. kliknąć w dany kontener prawym guzikiem i dodać nowego użytkownika czy komputer.



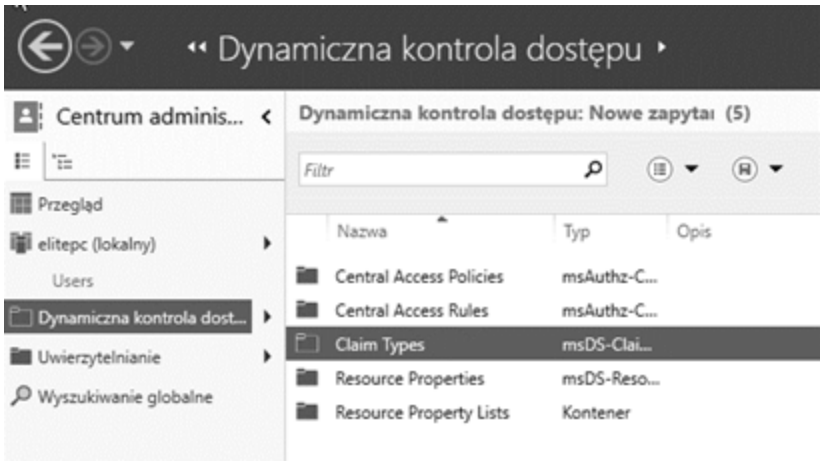
Zmianie uległy także kreatory. Teraz nie ma potrzeby przeglądania kilku zakładek jedna po drugiej, wszystkie właściwości zostały zebrane w postaci formularza.



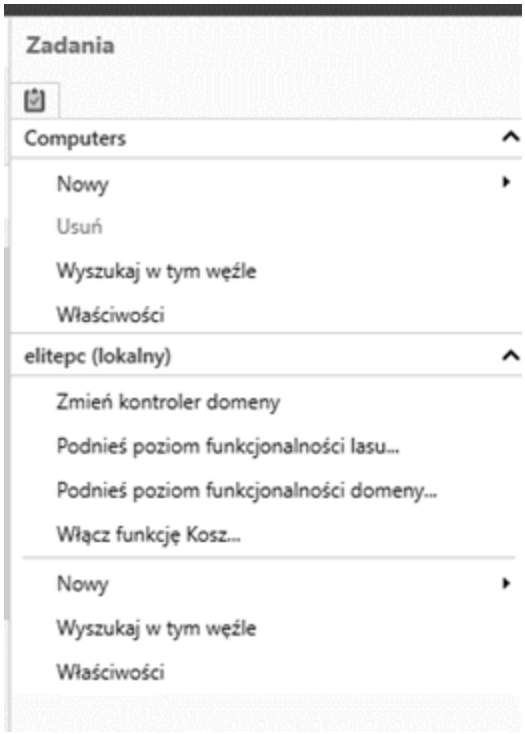
Na uwagę zasługuje także wyszukiwanie globalne, a właściwie ciekawa funkcjonalność, jaka się tam znalazła, tj. możliwość skonwertowania zapytania do formatu LDAP.



Wracając jednak do okna głównego nowej przystawki, warto zauważyć, iż pojawił się kontener Dynamiczna Kontrola Dostępu (Dynamic Access Control), który powiązany jest z autoryzacją bazującą na mechanizmie Claim, o którym będzie więcej w dziale 8.3. Na tą chwilę wystarczy wiedza, iż Central Access Policies odpowiada za polisy autoryzacji w metodzie Claim, Central Access Rules posiada w sobie reguły autoryzacyjne niezbędne przy budowaniu polis dostępu, Claim Types zawiera uzgodnienia (Claim) pomiędzy obiektem a atrybutami obiektu, Resource Properties to miejsce na zdefiniowane ustawienia zasobów używane przy autoryzacji typu Claim, natomiast Resource Property List to nic innego, jak listy własności zasobów używanych podczas autoryzacji Claim.

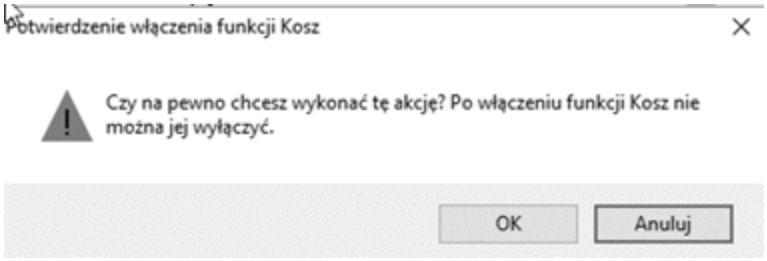


Warto teraz kliknąć w nazwę domeny i zerknąć na menu po prawej stronie.



Oprócz trzech opcji znanych z Windows Server 2008 R2, czyli Zmiany kontrolera domeny (Change domain controller) oraz Zwiększania poziomu funkcjonalności domeny, bądź lasu (Raise the domain functional level oraz Raise the forest functional level), pojawił się także Kosz dla Usługi Active Directory (Enable Recycle Bin). Po kliknięciu w niego pojawi

się komunikat o tym, że raz włączonego kosza nie można już wyłączyć. Należy to potwierdzić, klikając w OK.



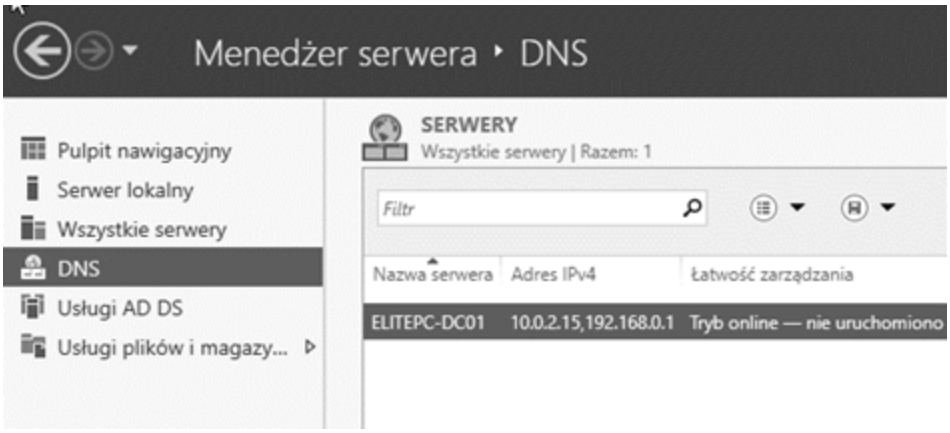
4. Serwer DNS

Działanie współczesnych sieci komputerowych byłoby niemożliwe bez użycia usługi DNS. To właśnie ona odpowiada za tłumaczenie nazw przyjaznych dla użytkowników na adresy IP. Dla przykładu, odwołując się do ulubionej domeny internetowej, to właśnie serwer DNS mówi komputerowi, z jakim adresem IP ten ma się połączyć. Tłumaczenie oczywiście działa w obydwie strony. Czytelnik z tego rozdziału dowie się, w jaki sposób Windows Server 2016 realizuje usługę DNS oraz jak nią zarządzać.

4.1. Zapoznanie z konsolą DNS Manager

Wraz z Active Directory automatycznie zainstalował się serwer DNS. Stało się tak, ponieważ Active Directory do

prawidłowego działania wymaga serwera nazw. Gdyby w sieci przed instalacją AD DS istniał już inny serwer DNS, najprawdopodobniej zostałby on użyty, w zależności od kroków, jakie zostałyby wybrane podczas instalacji AD DS. AD współpracuje tylko z serwerami hostowanymi w Windows Server.

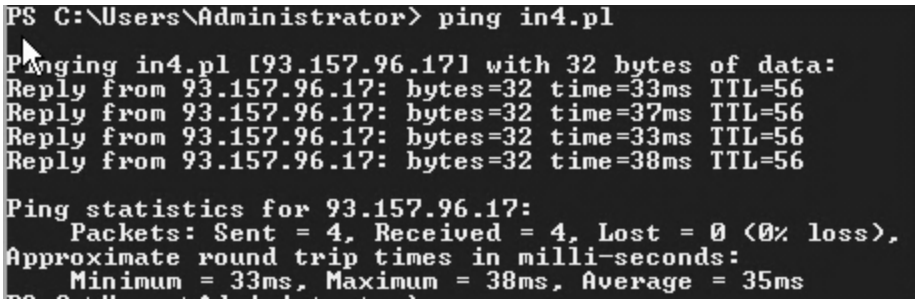


DNS (Domain Name System), czyli system nazw domenowych, to usługa zapewniająca zamianę adresów znanych użytkownikom na adresy, które staną się zrozumiałe dla urządzeń wchodzących w skład sieci komputerowej. Na przykład zamiast odwoływać się do komputera w domenie poprzez podanie adresu IP 192.168.1.xxx, będzie można napisać np. komputer01.Elitepc.pl. Na podobnej zasadzie działa cała globalna sieć. Aby sprawdzić, jaki adres IP kryje się pod daną nazwą, wystarczy wejść w konsolę PowerShell

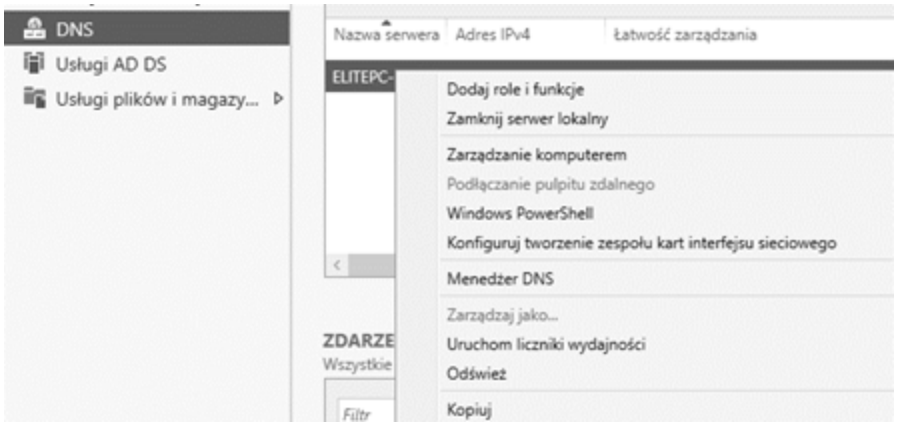
.

Wystarczy, że w konsoli, która się pojawi, zostanie podana komenda ping adres strony www. Z poniższego przykładu można się dowiedzieć, że wortal komputerowy

in4.pl posiada adres IP 195.242.117.52. Zamiast wpisywać w przeglądarce adres strony www jako in4.pl, można podać powyższy ciąg cyfr. Efekt będzie taki sam.



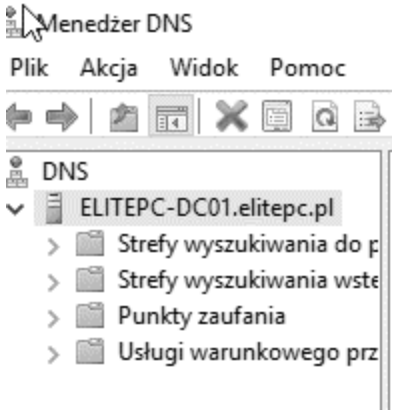
Ważną rzeczą, o której należy wspomnieć, jest to, iż komputery obce, niebędące częścią domeny, nie będą mogły się odwoływać do komputerów wewnątrz sieci adresem komputer01.Elitepc.pl. Natomiast komputery wewnątrz domeny nie tylko będą to potrafiły, ale jeszcze będą mogły korzystać z serwera DNS do tłumaczenia adresów internetowych. Jest to o tyle ważne, że przy dużych sieciach znacznie minimalizuje obciążenie łącza internetowego. Przechodząc do konsoli zarządzania usługą, po znalezieniu na liście serwera, należy kliknąć na nim prawym przyciskiem myszy, a następnie wybrać Menadżer Serwera DNS (DNS Manager).



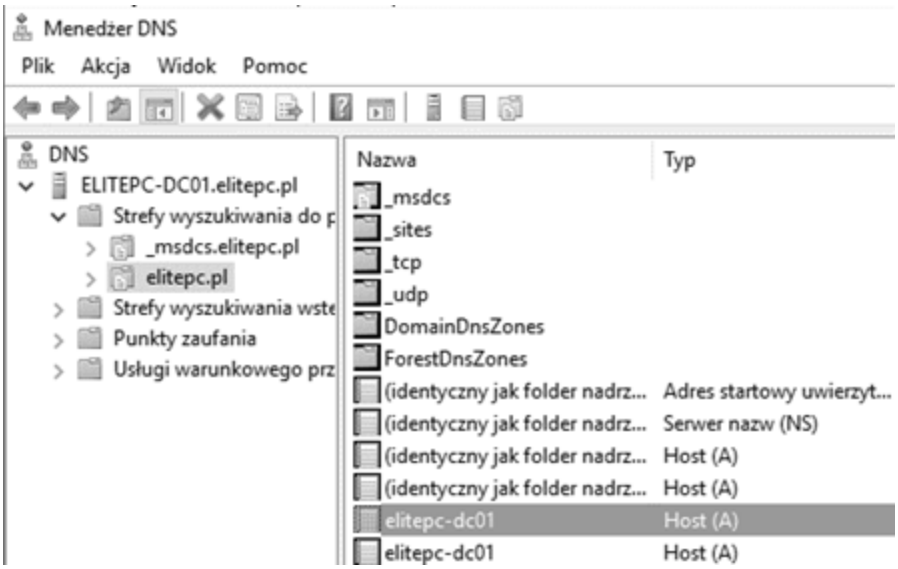
Usługa DNS podzielona jest na dwie strefy:

- wyszukiwania do przodu,
- wyszukiwania wstecznego.

Strefa wyszukiwania do przodu jest mniej więcej tym, co wcześniej zostało opisane i jest już ona skonfigurowana. Natomiast strefa wyszukiwania wstecznego działa, jak sama nazwa wskazuje, w stronę przeciwną, czyli posługując się przykładem, zamieni adres IP 195.242.117.52 na in4.pl. DNS działa tylko wewnątrz sieci.

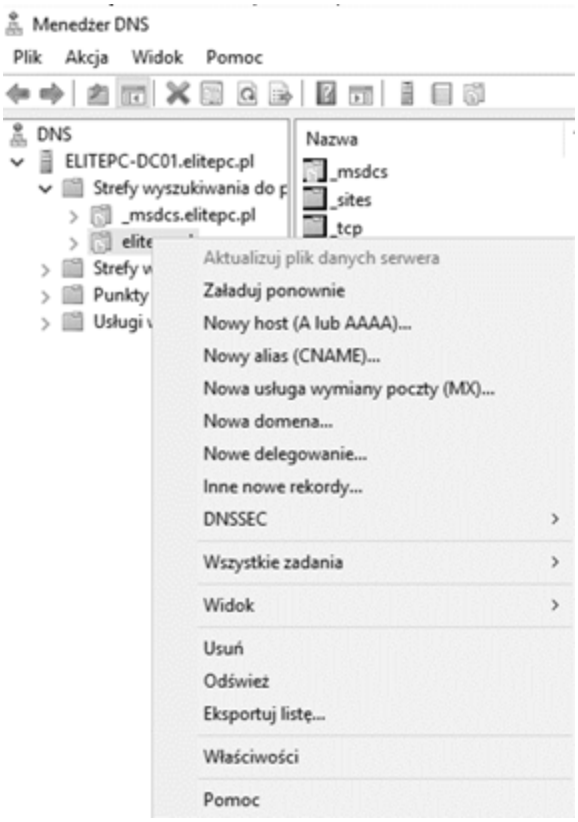


Należy rozwinąć strefę przewijania do przodu, a następnie zaznaczyć domenę, na serwerze przykładowym będzie to ElitePC.pl. Warto zwrócić uwagę, że po prawej stronie znajdują się różnego rodzaju wpisy, np. zaznaczony wpis typu A, czyliHost(A), dla kontrolera domeny definiuje nam to, że nazwa ElitePC-DC01 w sieci lokalnej będzie jednoznaczna z adresem IP 192.168.1.1.

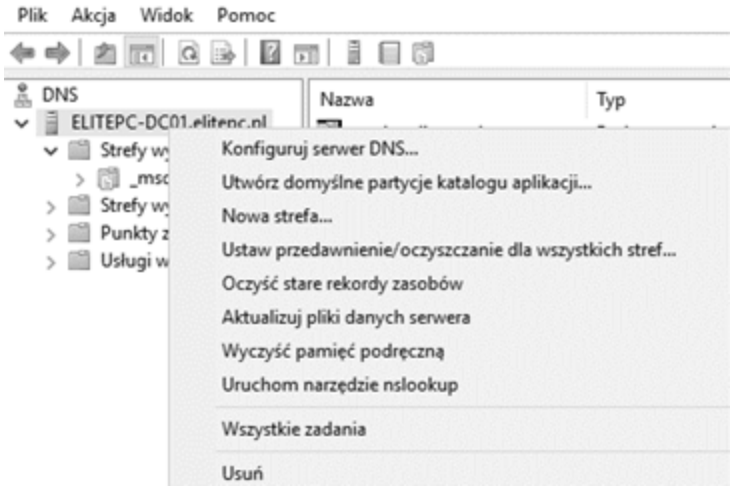


4.2. Ręczna konfiguracja strefy DNS

Na potrzeby ćwiczenia zostanie skasowana główna strefa wyszukiwania do przodu, żeby pokazać jak ją ręcznie utworzyć. Należy kliknąć na niej prawym przyciskiem myszy i wybrać opcję Usuń (Delete).

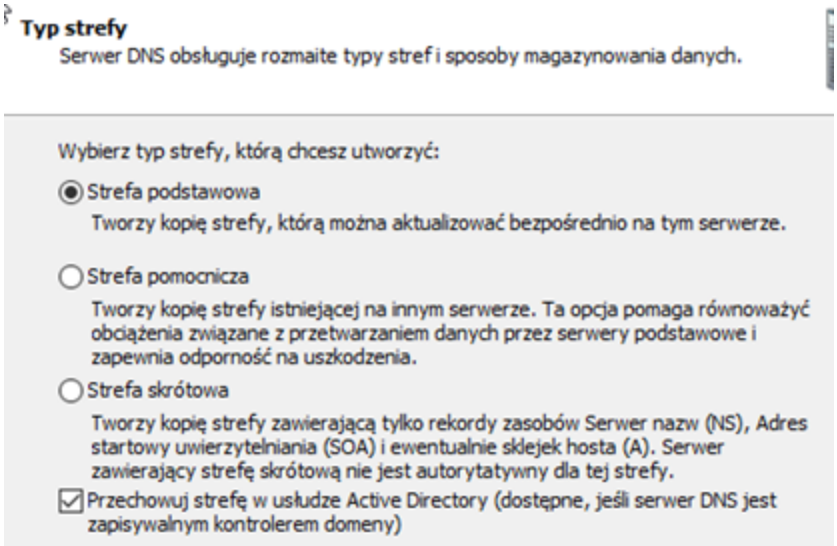


Następnie konieczne jest kliknięcie w nazwę serwera i wybranie opcji Nowa strefa (New Zone).

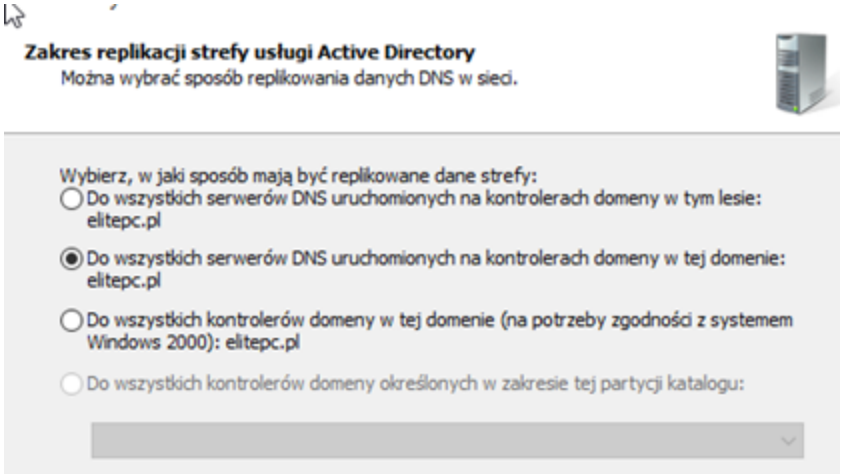


Otworzy się kreator, w którym stronę powitalną należy pominąć, klikając w Dalej (Next).

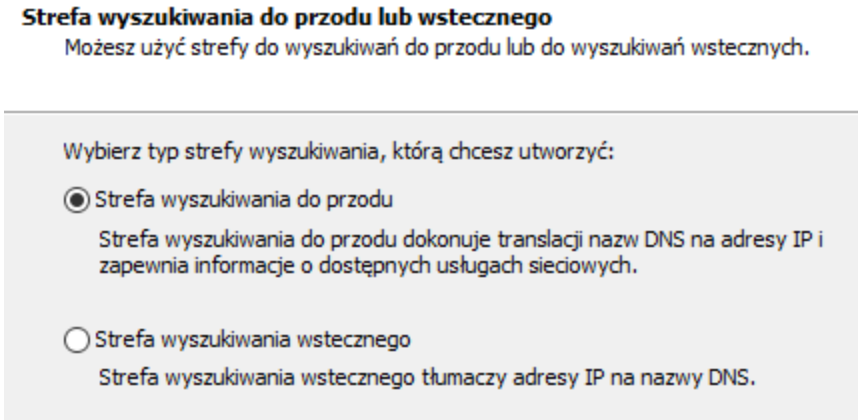
Kolejna plansza pozwoli wybrać rodzaj strefy. W tym przypadku zostanie wybrana Strefa podstawowa (Primary Zone), ponieważ serwer jest główną maszyną w sieci. Gdyby miał zostać zainstalowany dodatkowy serwer, np. zapasowy lub do zbilansowania obciążenia sieciowego, zostałaby wybrana Strefa pomocnicza (Secondary Zone). W lokalizacjach niezabezpieczonych najlepsza będzie Strefa skrótowa (Stub Zone). Jako że serwer pełni jednocześnie rolę kontrolera domeny, można wybrać opcję Przechowywanie strefy w usłudze Active Directory (Store the zone in Active Directory). Należy kliknąć przycisk w Dalej (Next).



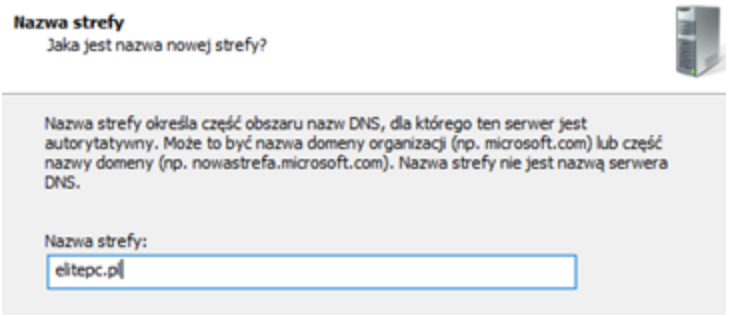
Kolejna karta określa sposób replikacji danych DNS. Można przekazywać rekordy W całym lesie (To all DNS servers running on domain controllers in this forest), jedynie W obrębie domeny (To all DNS servers running on domain controllers in this domain) (co zostanie wybrane), bądź do Wszelkich kontrolerów domeny (To all domain controllers in this domain (for Windows 2000 compatibility)) (wymagane w przypadku starszych serwerów). Należy kliknąć Dalej (Next).



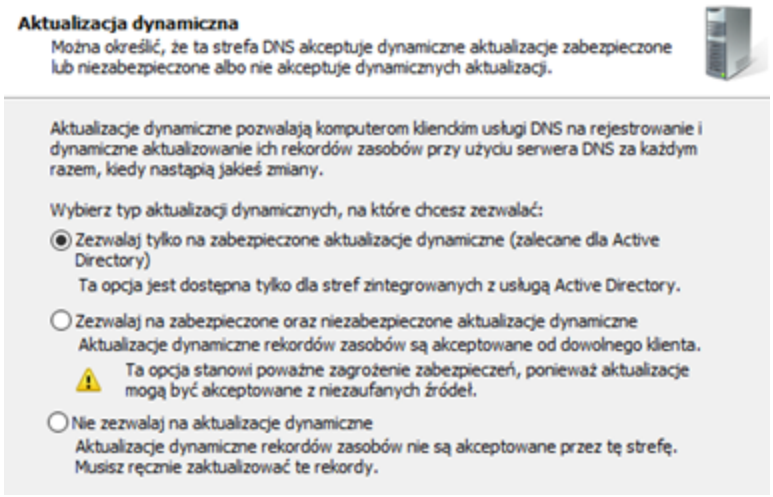
Następnie należy wybrać, czy tworzona jest strefa wyszukiwania do przodu czy wstecznego. Zostanie wybrana opcja pierwsza.



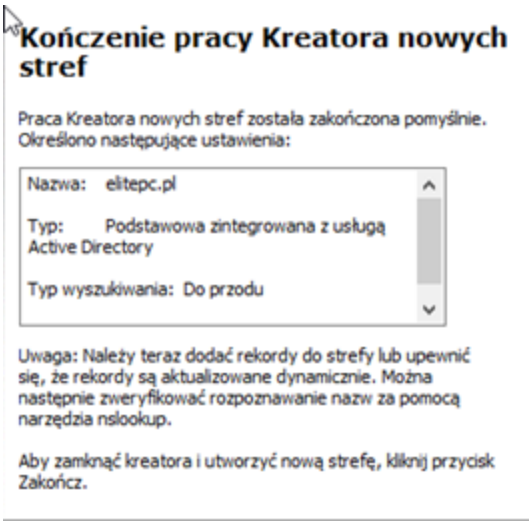
Ponieważ jest to główny serwer, naturalną nazwą strefy będzie elitepc.pl.



Na kolejnej planszy zostaną pozostawione opcje domyślne. Należy kliknąć przycisk Dalej (Next). Ustawienia te zostaną zmienione za chwilę.

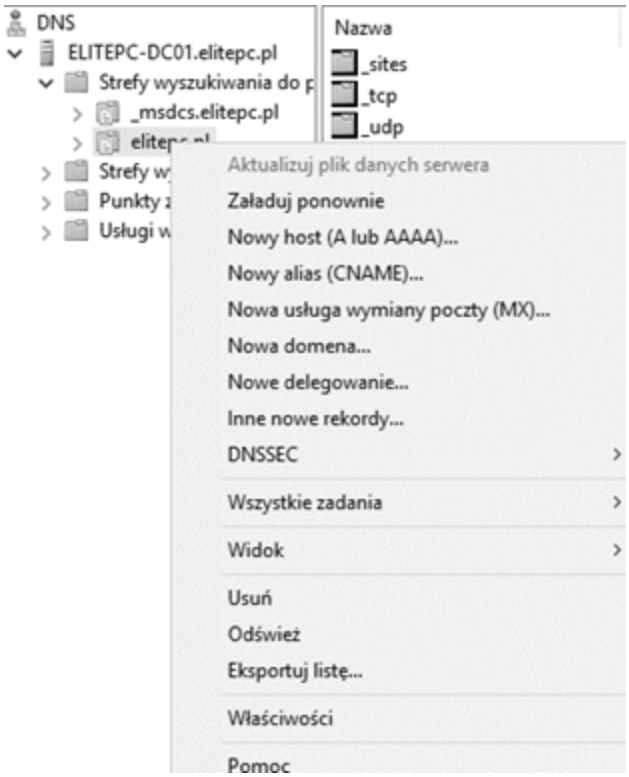


Na ostatniej planszy należy kliknąć w Zakończ (Finish).

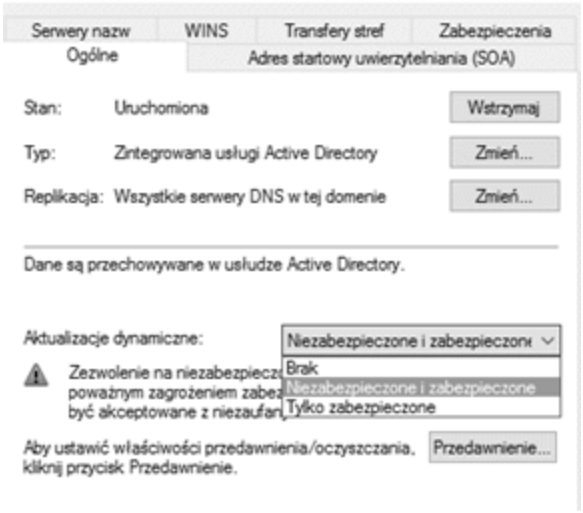


4.3. Zarządzanie serwerem DNS

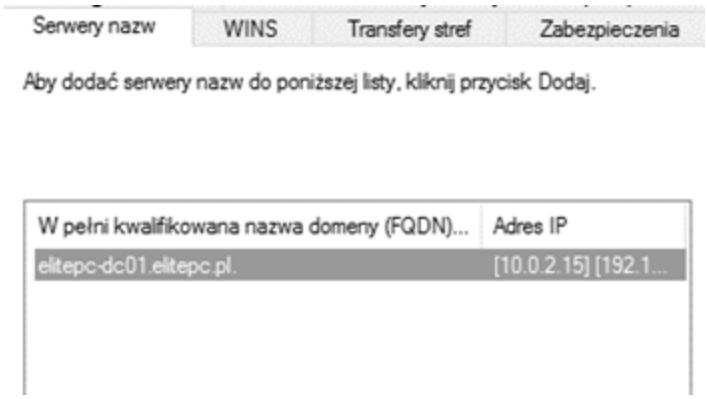
Usługa DHCP ma być ustawiona tak, aby aktualizowała przy okazji przyznania adresu rekordy DNS. Doda ona rekord A oraz PTR dla komputerów korzystających z sieci. Pojawią się one na liście pod serwerem. Gdyby jednak korzystano ze starszej wersji systemu Windows lub istniały jakieś inne problemy, można kliknąć w nazwę domeny, np. ElitePC.pl, i wybrać Właściwości (Properties).



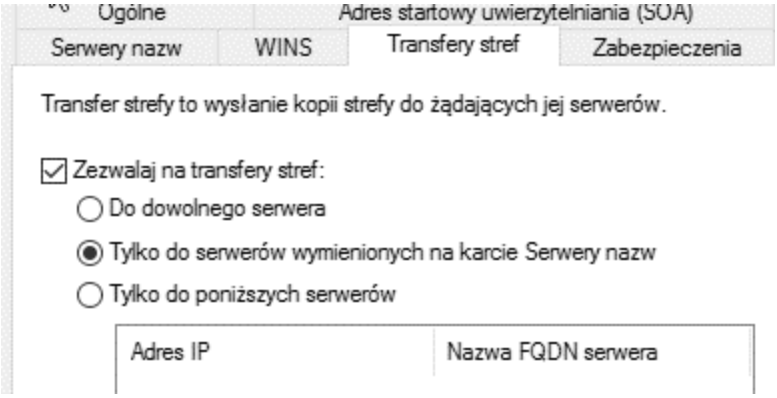
Niekiedy, choć nie jest to zalecane, konieczna będzie zmiana aktualizacji dynamicznych na Niezabezpieczone i zabezpieczone (Nonsecure and secure).



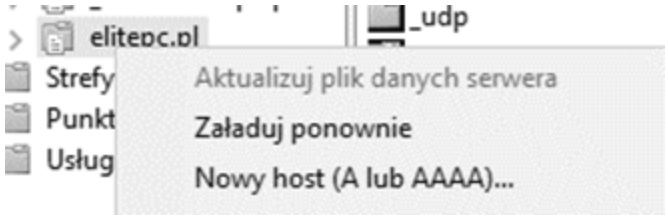
W zakładce Serwery Nazw (Name Servers) można dodać inne działające w sieci serwery DNS.



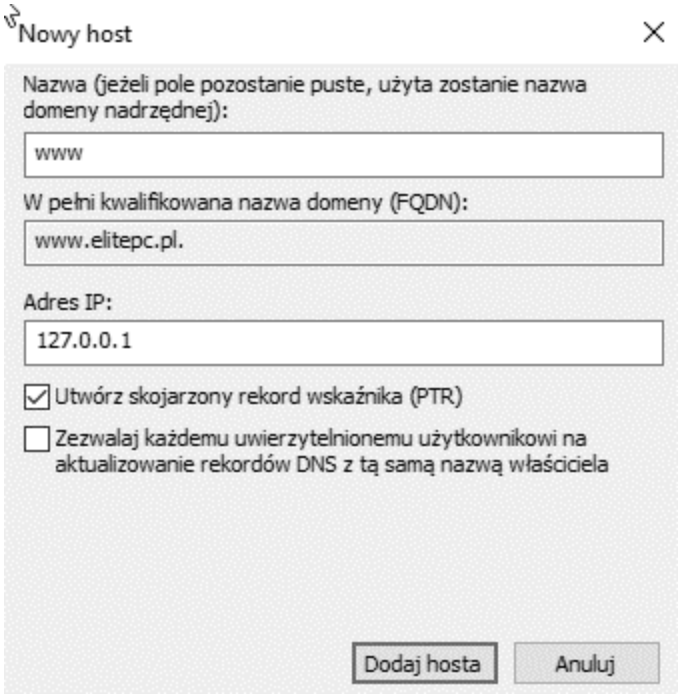
Dzięki temu można następnie w zakładce Transfer Strefy (Zone transfer) określić ustawienia tak, aby wszelkie zmiany w tym serwerze DNS były propagowane do innych serwerów z poprzedniej karty Serwery Nazw (Only to servers listed on the Name Servers tab). Inną możliwością jest Transfer strefy do dowolnego serwera w sieci (To any server) lub Dodanie serwerów poprzez podanie ich adresów IP (Only to the following servers). Ze względów bezpieczeństwa, jeżeli istnieje tylko taka możliwość, zaleca się dzielenie rekordami DNS wyłącznie z członkami domeny.



Oczywiście można dodawać także nowe rekordy ręcznie. Do najbardziej popularnych należą rekordy A, AAAA, CNAME, MX i NS. Host A, czyli rekord adresu, pozwala przypisać ręcznie dowolną nazwę pod dany adres IP jakiegoś urządzenia sieciowego.

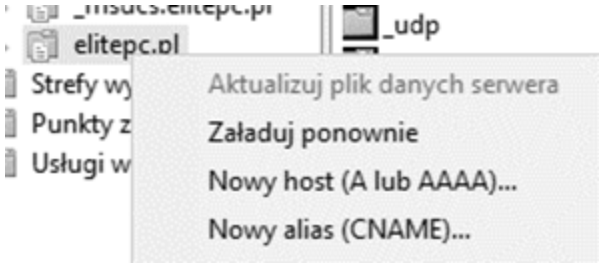


Wystarczy podać nazwę hosta, a FDQN zostanie sam wygenerowany oraz adres IP, na który ma on wskazywać. Stworzenie rekordu PTR tworzy wpis odwrotny dla Hosta A, czyli wpis w strefie wyszukiwania wstecznego. Należy pamiętać o tym, że strefa wyszukiwania wstecznego musi być utworzona, aby PTR powstał.

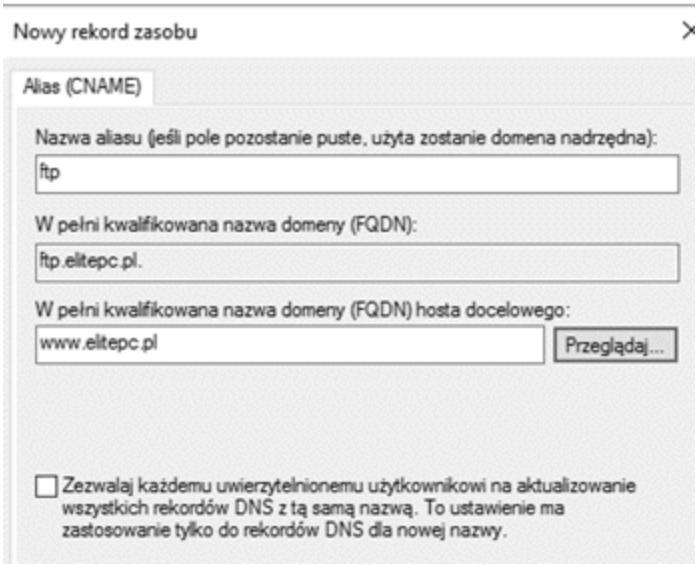


Host AAAA, czyli rekord adresu Ipv6, pozwala przypisać ręcznie dowolną nazwę pod dany adres IPv6 jakiegoś urządzenia sieciowego. CNAME tworzy alias dla istniejącego już wpisu, czyli wiele nazw może wskazywać na ten sam adres IP. Zaleca się tworzyć rekordy CNAME zamiast duplikować rekordy A, choćby z powodów ilości pamięci w bazie danych. Rekord MX jest używany do mapowania

serwerów poczty, a NS serwerów DNS. Przechodząc przez kreator, pojawi się rekord PTR, zwany rekordem wskaźnika, który pozwala na implementację strefy wyszukiwania wstecznego. Dla przykładu zostanie utworzony rekord CNAME dla kontrolera domeny, który się przyda w kolejnych działach. W tym celu należy kliknąć prawym przyciskiem myszy na nazwie domeny i wybrać Nowy Alias (CNAME) (New Alias (CNAME)).

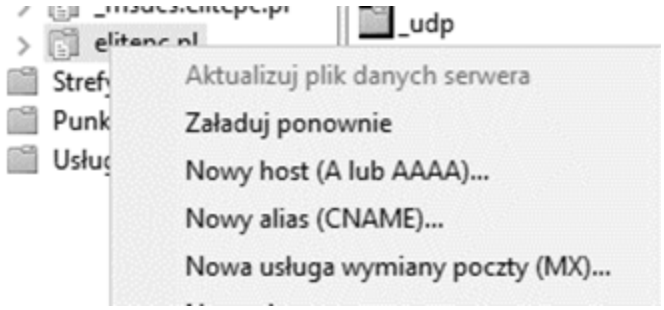


Nazwa aliasu jest dowolna, dla przykładu zostanie wpisane „FTP”. Należy także podać w pełni kwalifikowaną nazwę domeny dla hosta docelowego. Innymi słowy, po prostu wskazać rekord A komputera, do którego alias ma się odwoływać. Sposób składania takiego adresu wydaje się dość logiczny, jednak w przypadku problemów można użyć przycisku Przeglądaj (Browse) i wybrać odpowiedni komputer z listy.

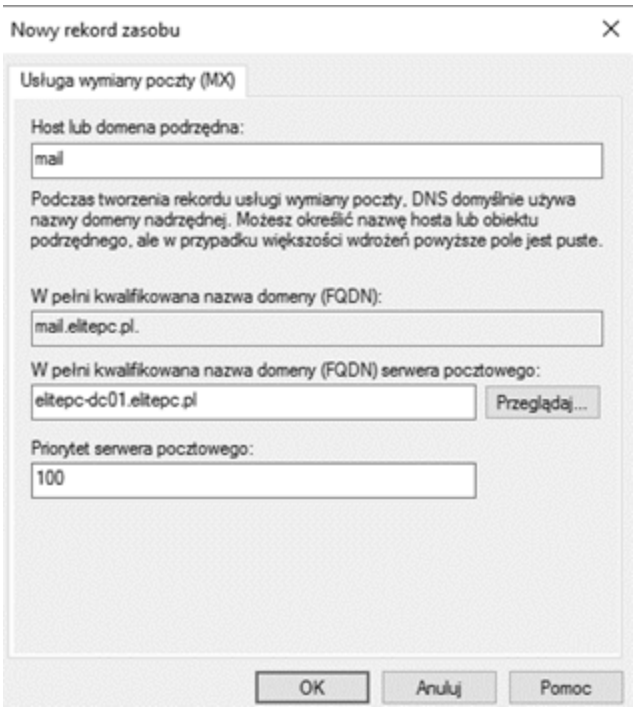


Utworzone zostaną także aliasy dla skrótów WWW oraz VPN. Pozwolą one użytkownikom łączyć się z serwerem po podaniu adresu www.Elitepc.pl, vpn.Elitepc.pl, ftp.Elitepc.pl, elitepc.pl. Dzięki temu nie tylko będzie to wyglądać bardziej profesjonalnie przy podawaniu różnego rodzaju danych do konfiguracji, ale także poprawi intuicyjność rozwiązania, mimo że tak naprawdę połączenie następuje cały czas z jednym i tym samym komputerem. Co więcej, gdyby każda rola serwera, tak jak ma to miejsce w profesjonalnych zastosowaniach, była zrealizowana na osobnych komputerach, konieczne byłoby utworzenie takich rekordów.

Rekordy MX – wymiany poczty, przeznaczone są dla serwerów pocztowych, np. Microsoft Exhange.

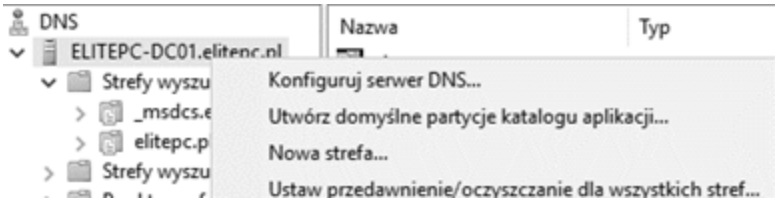


Ich konfiguracja analogiczna jest do aliasów z tym, że posiadają one jeszcze pole na określenie priorytetu serwera pocztowego. Zaleca się priorytety zwiększać co 10, jeśli oczywiście jest taka możliwość, w przedziale 1 do 100. Serwer o największym priorytecie będzie używany przez użytkowników sieci tak długo, aż nie zostanie on przeciążony, bądź nie ulegnie awarii.

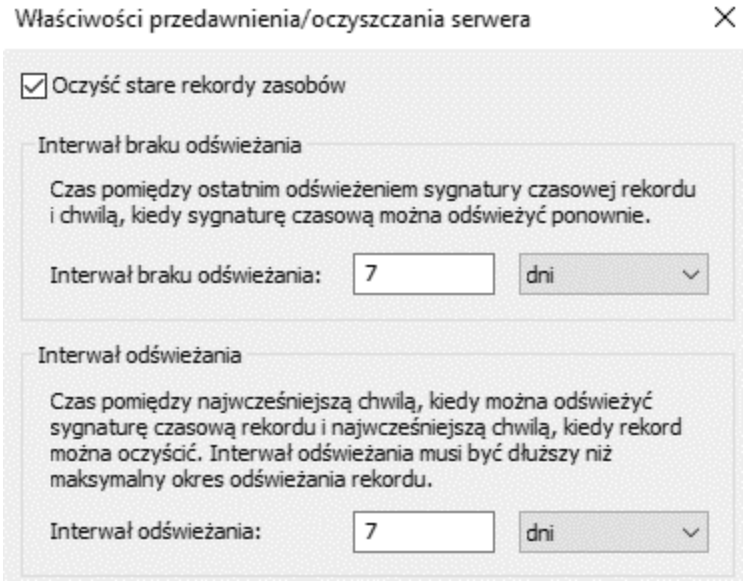


Serwer posiada także opcje oczyszczania samego siebie z nieaktualnych rekordów. Wystarczy na serwerze kliknąć

prawym klawiszem myszy i wybrać opcję związaną z oczyszczaniem (Set Aging/Scavening for All Zones…).



W oknie, które się pojawi, należy wybrać, jak długo nieodświeżony rekord może pozostać w serwerze DNS oraz co jaki czas serwer ma weryfikować swoje rekordy.



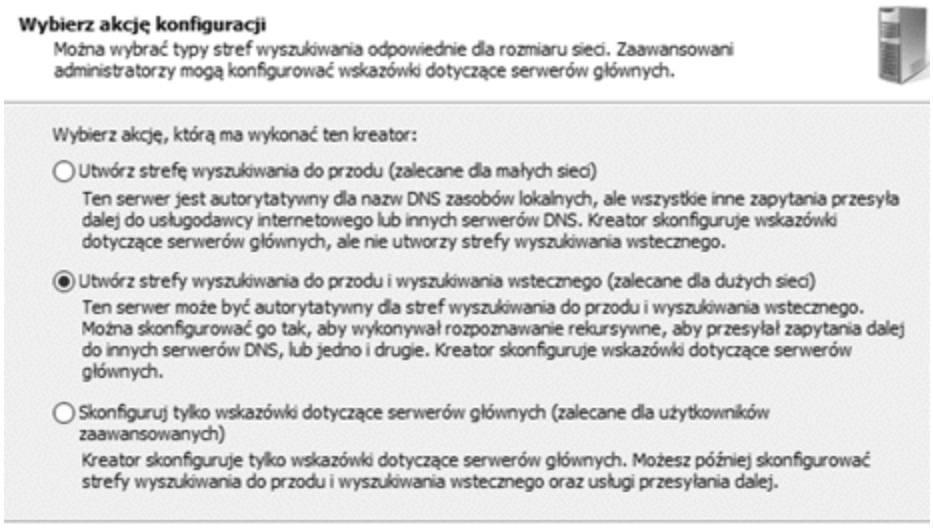
4.4. Zapasowy serwer DNS

Naturalnie server DNS można zainstalować niezależnie od Active Directory, np. na osobnym serwerze, do czego się zachęca, jeśli są ku temu odpowiednie środki. Najbezpieczniej i najwydajniej sieć będzie pracowała, jeżeli

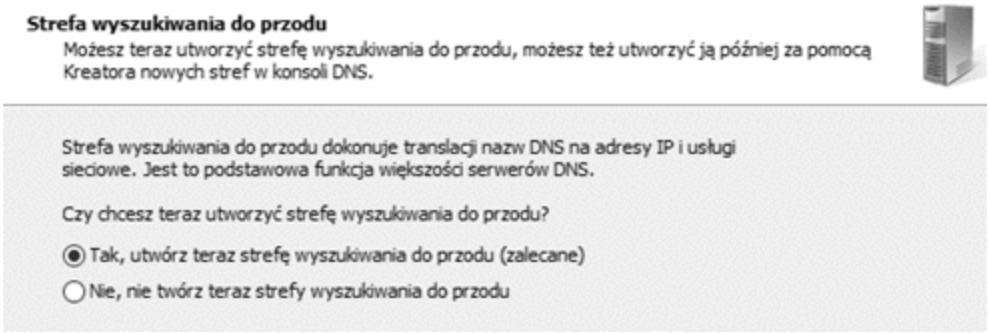
na pojedynczym serwerze będzie jak najmniej zainstalowanych ról. Należy kliknąć na nazwie serwera prawym przyciskiem myszy i wybrać opcję Skonfiguruj serwer DNS (Configure a DNS Server).

Kartę powitalną można pominąć, klikając przycisk Dalej (Next).

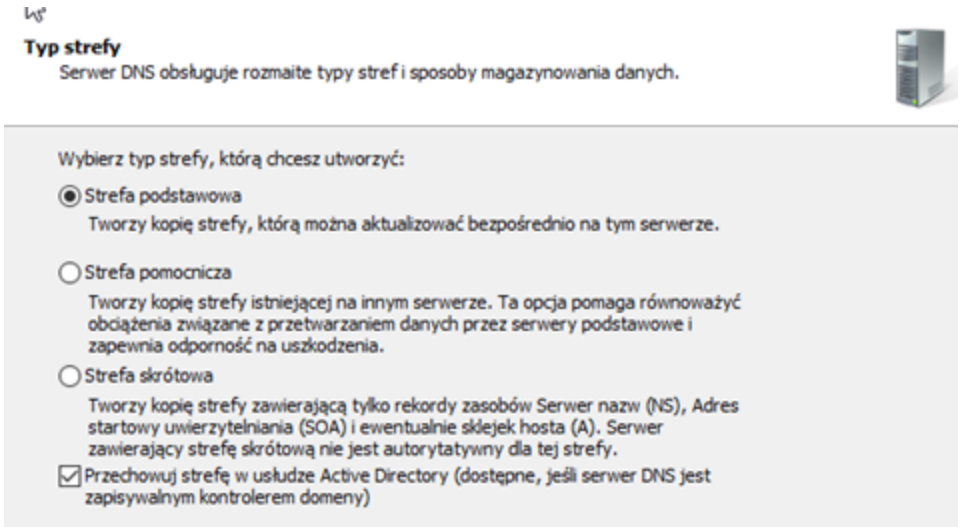
Do wyboru są trzy możliwości, z czego większość pewnie najbardziej zainteresują dwie pierwsze. Jedną z nich jest Stworzenie strefy wyszukiwania do przodu (Create a forward lookup zone), która świetnie sprawdza się w małych i średnich firmach. Lokalne zapytania będą rozwiązywane przez lokalny DNS, natomiast te spoza sieci będą przekazywane do serwerów dostawcy Internetu. Dla dużych firm zaleca się Stworzenie strefy wyszukiwania do przodu oraz do tyłu (Create forward and reverse lookup zones). Serwer ten jest w pełni autorytatywny. Aby prześledzić dokładnie kreator konfiguracyjny, należy wybrać opcję drugą.



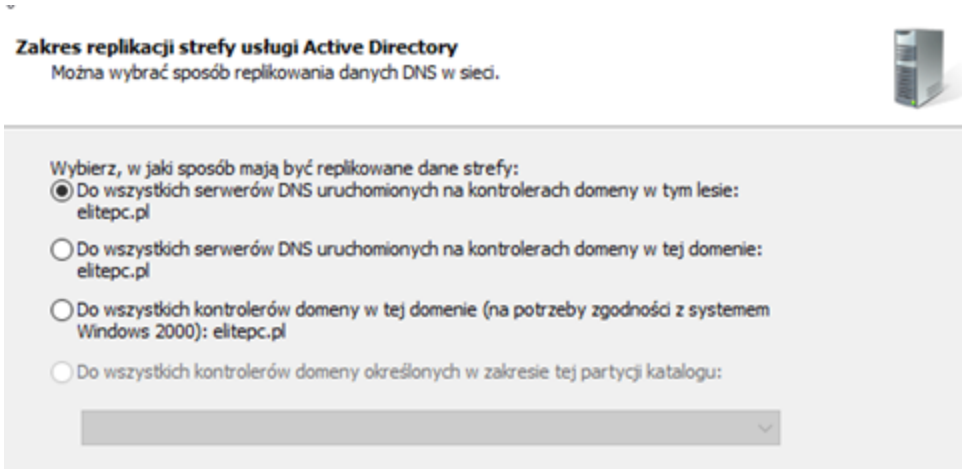
Na kolejnej karcie należy wybrać opcję zalecaną (Yes, create a forward lookup zone now), ponieważ ma zostać skonfigurowana strefa wyszukiwania do przodu.



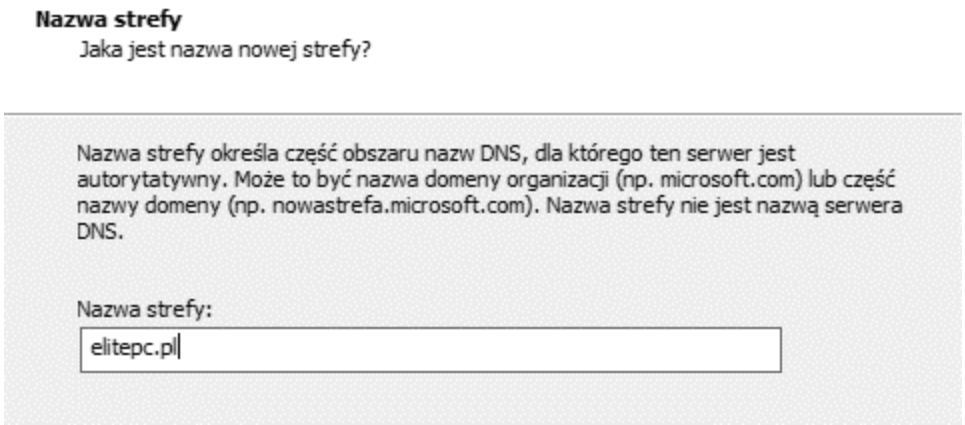
Jako że jest to pierwszy serwer, stworzona zostanie Strefa główna (Primary Zone). Gdyby to był serwer zapasowy, zostałaby wybrana opcja druga. Zaznaczona także zostanie opcja Przechowanie strefy DNS w Active Directory (Store the zone in Active Directory).



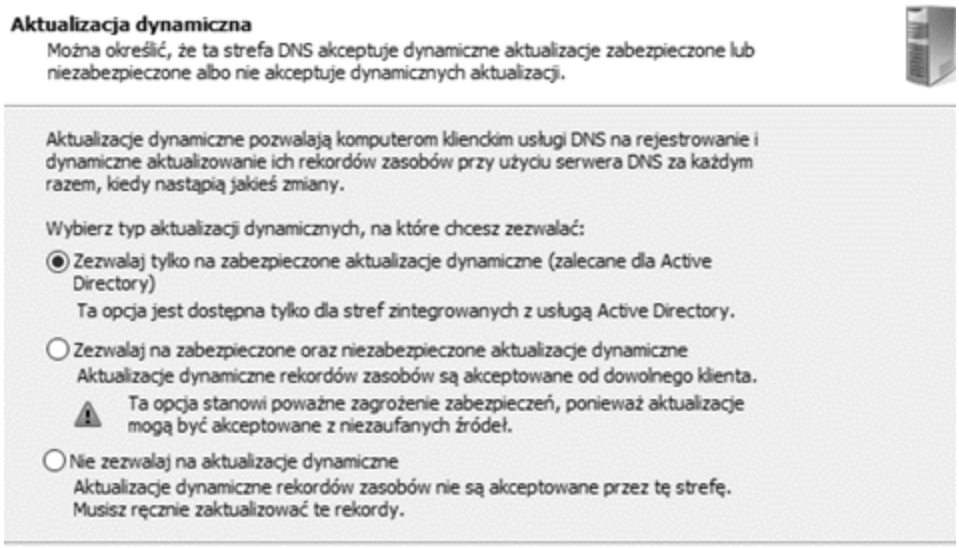
Następnie należy określić metodę replikowania danych. Rekordy można propagować do wszystkich serwerów w lesie, tylko w domenie lub w partycji domenowej.



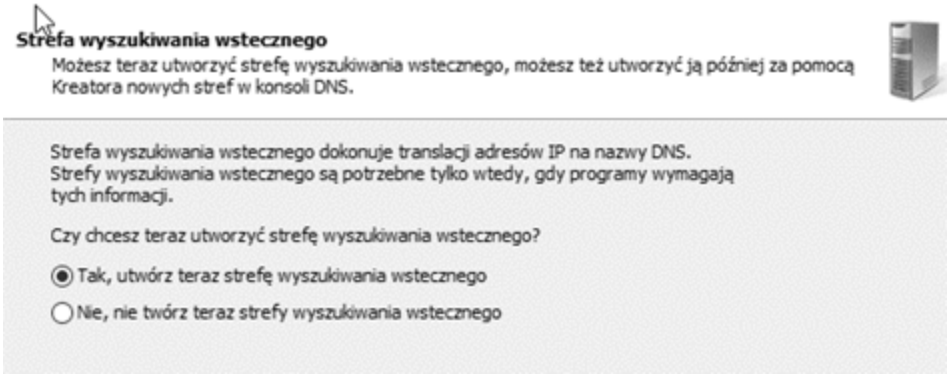
W kolejnym kroku należy podać nazwę strefy.



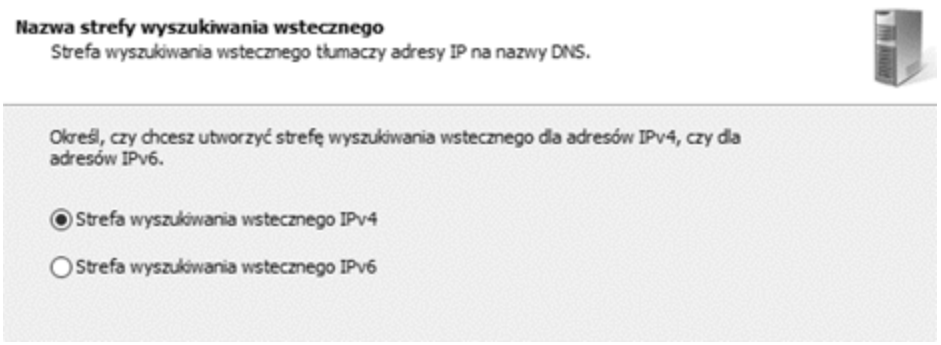
Należy określić opcje związane z aktualizacjami dynamicznymi, o których mowa była już wcześniej.



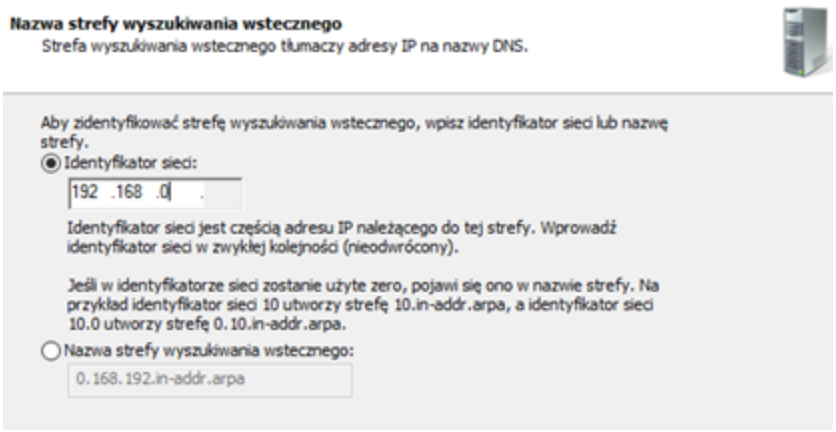
W kolejnym oknie definiuje się, czy ma zostać skonfigurowana strefa wyszukiwania wstecznego. Należy zaznaczyć Tak (Yes, create a reverse lookup zone now) i kliknąć w Dalej (Next).



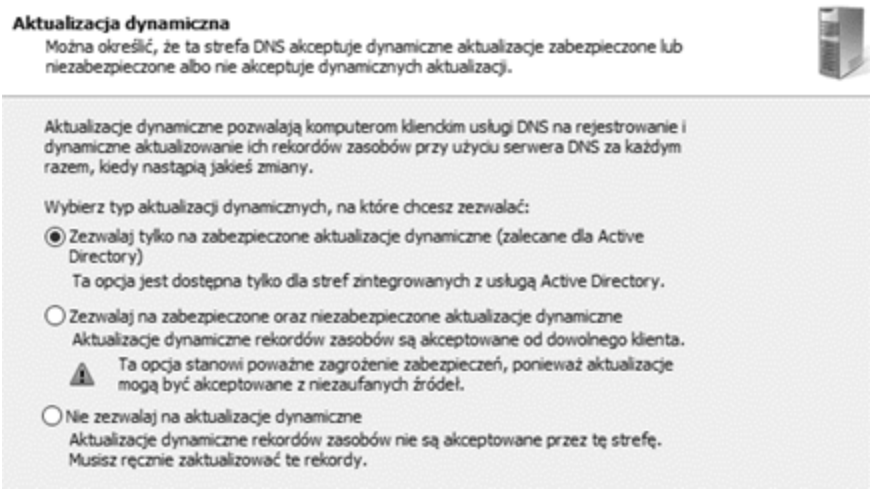
Kolejne trzy kroki są analogiczne do strefy wyszukiwania do przodu. Dochodzi się tak do planszy, na której należy zdefiniować, czy strefa ma dotyczyć adresów IPv4 (IPv4 Reverse Lookup Zone) czy IPv6 (IPv6 Reverse Lookup Zone).



Teraz należy zdefiniować adresację IP, jaka funkcjonuje w sieci.

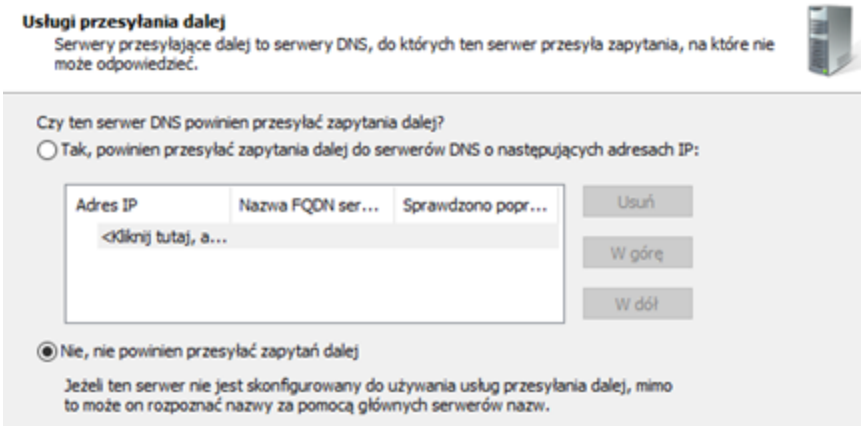


Po raz kolejny należy skonfigurować aktualizacje dynamiczne.



W następnym kroku definiuje się, czy serwer ma przekazywać zapytania, których nie może rozwiązać, do

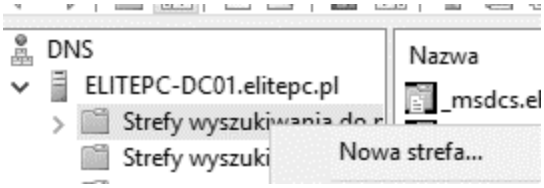
innego serwera, a jeśli tak, to do jakiego. W przypadku wykonywanego ćwiczenia, przekazywanie zapytań dalej nie jest wymagane.



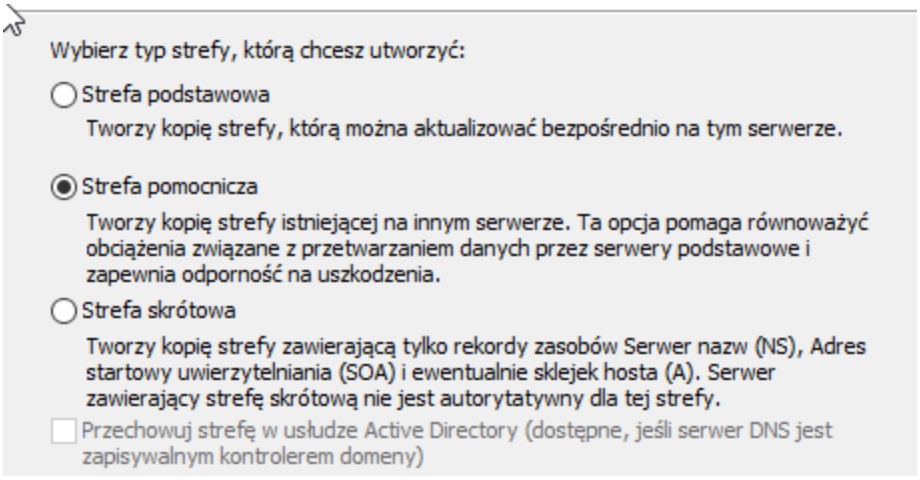
Był to ostatni krok instalacji. Na karcie podsumowującej wystarczy kliknąć Zakończ (Finish).

Jeżeli ma istnieć zapasowy server DNS, należy posiadać inny komputer z systemem Windows Server. Po zainstalowaniu na nim roli serwera DNS, należy w konsoli

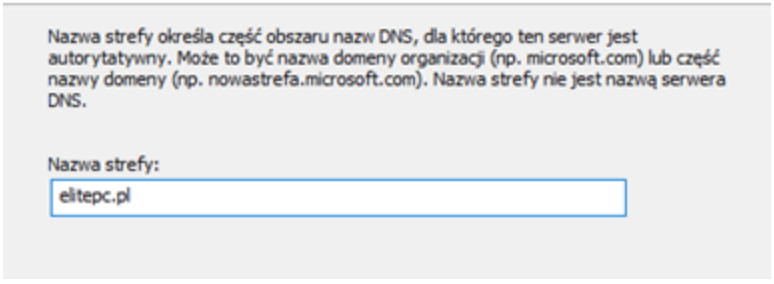
DNS Manager kliknąć prawym klawiszem myszy w strefę wyszukiwania i wybrać Nowa strefa (New Zone).



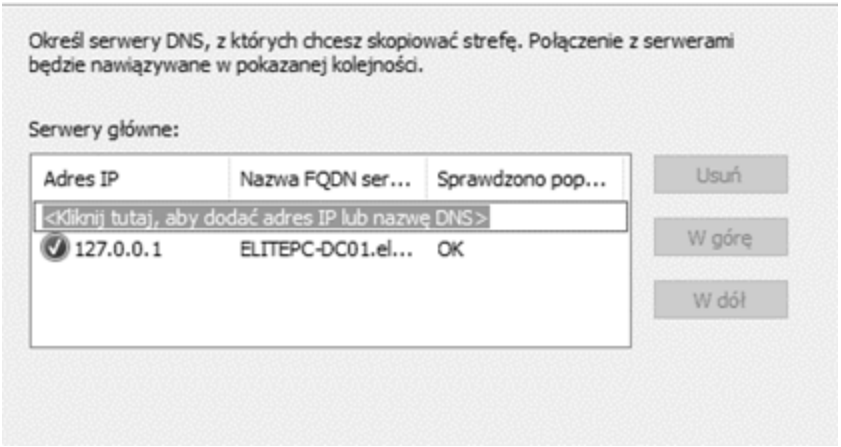
W kreatorze należy tym razem wybrać Strefa zapasowa (Secondary Zone). Dzięki temu nie tylko obciążenie serwera DNS będzie równoważone, ale także, w razie awarii jednego serwera, dane nie zostaną utracone, a jego rolę przejmie serwer zapasowy.



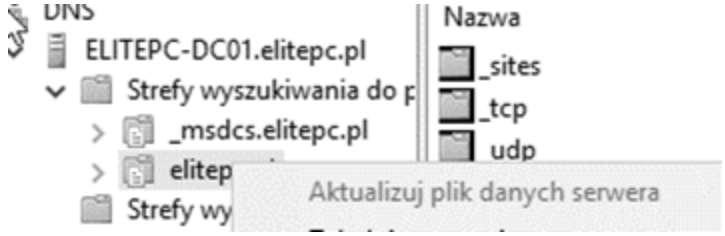
Należy wybrać odpowiednią nazwę strefy. Jest to o tyle ważne, że jeśli jest się w posiadaniu kilku domen, można duplikować jedynie porcje danych, a nie całą zawartość serwera DNS.



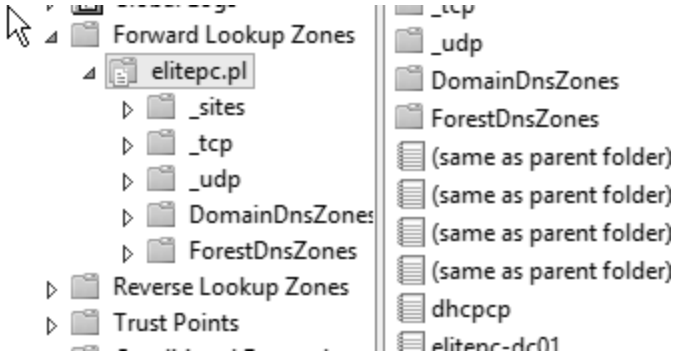
W kolejnym oknie należy podać adres IP komputera, na którym znajduje się już działający serwer DNS.



Na karcie podsumowującej należy wybrać Zakończ (Finish). Trzeba pamiętać, że serwer główny musi mieć we właściwościach ustaloną zgodę na transfer strefy do serwera docelowego. Gdy to zostanie wykonane i wstępna synchronizacja zostanie wymuszona opcją Transferuj z serwera głównego (Transfer From Master) z menu kontekstowego, które jest dostępne po kliknięciu prawym przyciskiem myszy w nazwę domeny.



Po synchronizacji rekordy z głównego serwera DNS powinny pojawić się na serwerze zapasowym.

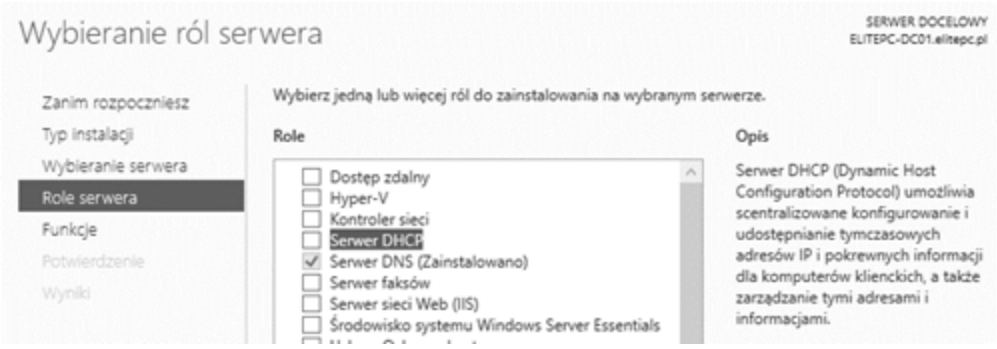


5. Serwer DHCP

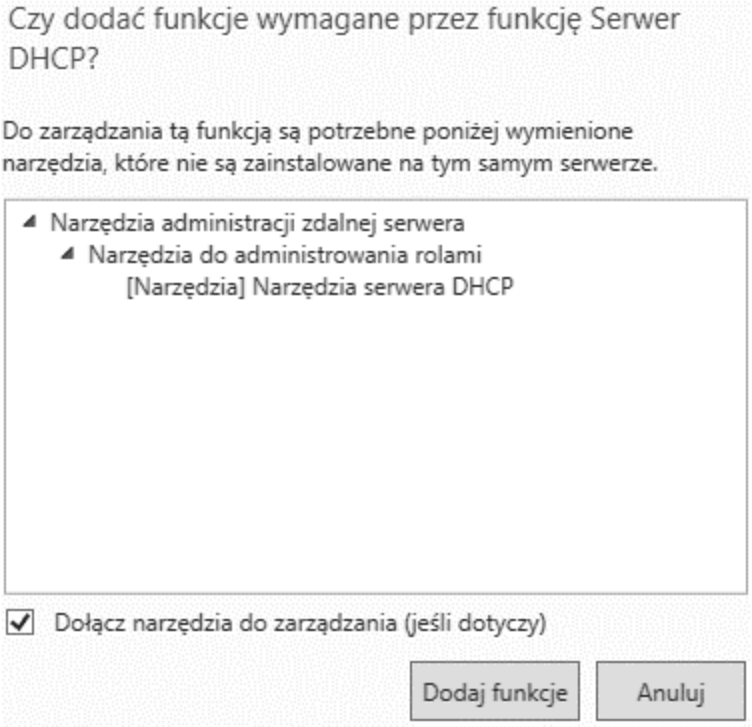
Serwer DHCP mówiąc kolokwialnie, przydziela adresy IP każdemu komputerowi, który się uruchomi podłączony do danej sieci. Jest to fundamentalny element każdej struktury sieciowej. Jedną z nowości w systemie Windows Server 2016 jest wprowadzenie funkcjonalności nazwanej polityką serwera DCHP (DHCP Policy). Czytelnik w tym dziale dowie się, jak zainstalować i zarządzać serwerem DHCP.

5.1. Instalacja pierwszego serwera DHCP

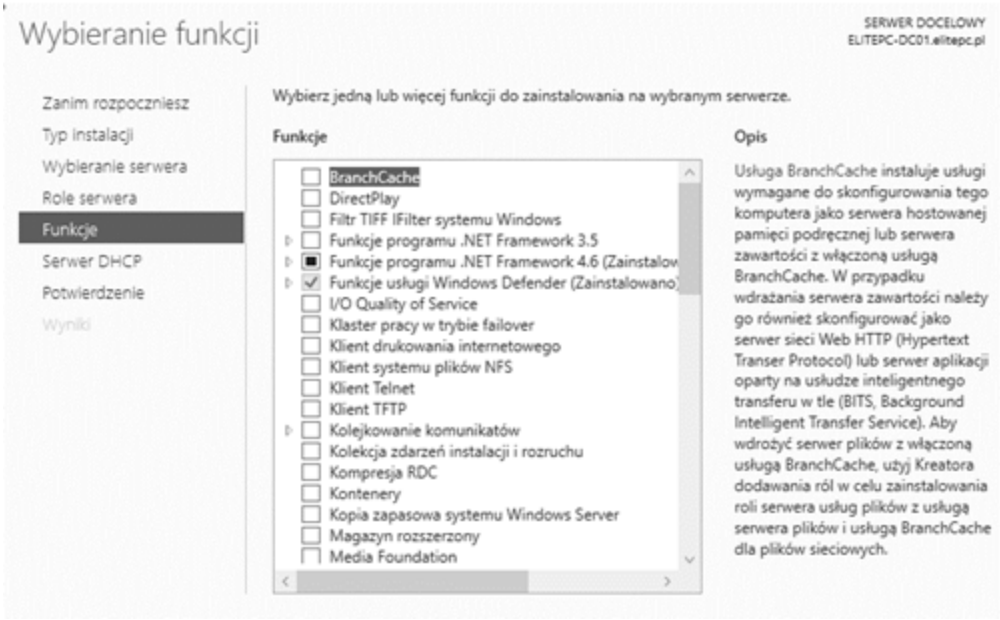
Podobnie jak w przypadku innych ról, instalację serwera DHCP również rozpoczyna się z poziomu Menadżera Serwera (Server Manager). Żeby go zainstalować, należy wybrać w kreatorze ról Serwer DHCP (DHCP Server) i kliknąć w Dalej (Next).



Następnie trzeba zaakceptować instalację wszelkich dodatkowych wymaganych funkcji.

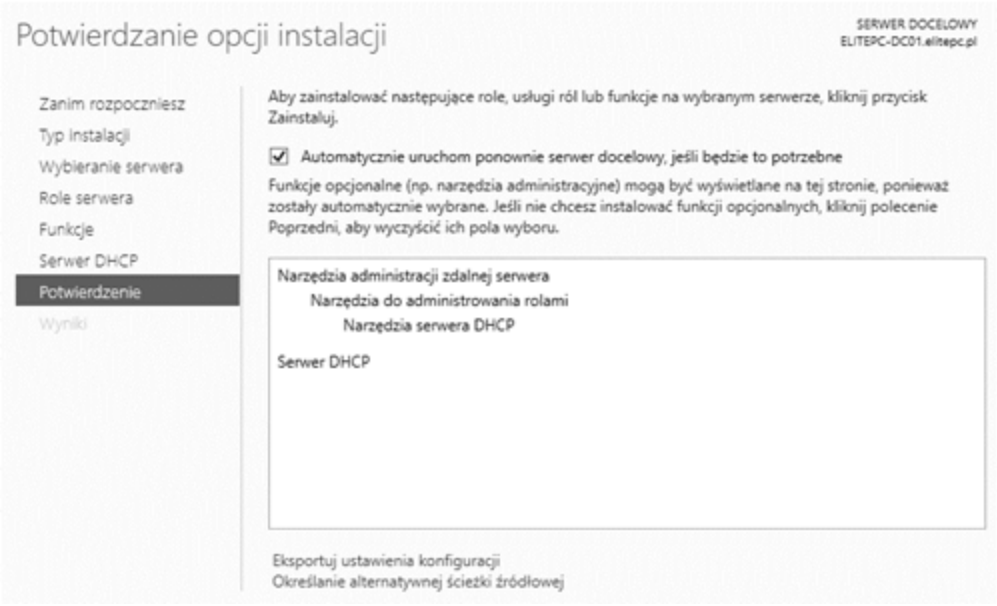


Na kolejnej planszy należy kliknąć Dalej (Next).

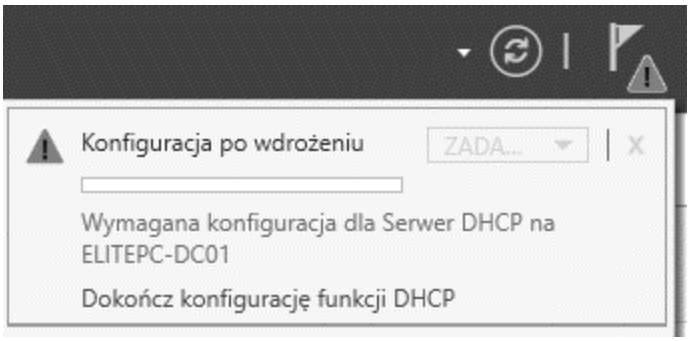


Na kolejnej planszy należy kliknąć Dalej (Next).

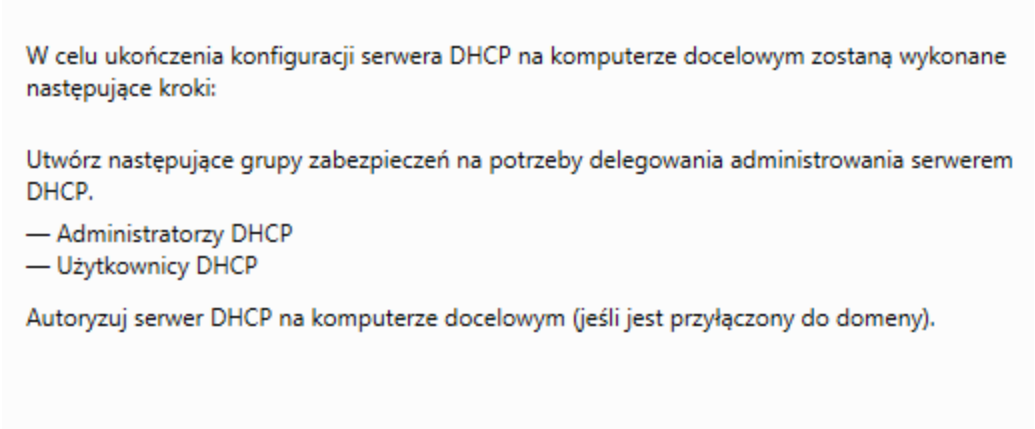
Na ostatniej karcie podsumowującej należy zaznaczyć opcję Uruchom ponownie serwer docelowy, jeśli wymagane (Restart the destination server automatically if required), aby w razie potrzeby serwer sam uruchomił się ponownie, a następnie należy kliknąć w Zainstaluj (Install).



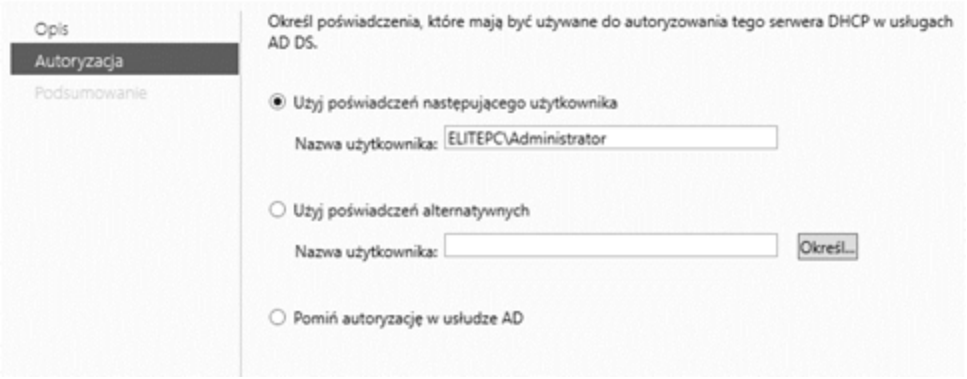
Po ponownym uruchomieniu komputera i wejściu do konsoli Menadżer serwera (Server Manager) w centrum akcji można zauważyć, że niezbędna jest dodatkowa konfiguracja serwera DHCP. Należy więc kliknąć w Dokończ konfigurację Konfigurację serwera DHCP (Complete DHCP Configuration).



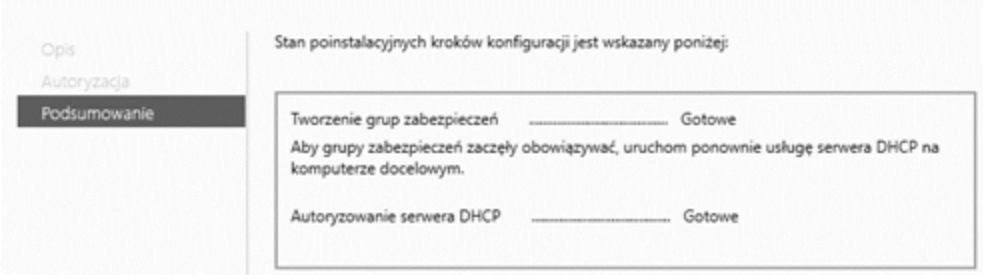
Pojawi się kreator postinstalacyjny. Jego zadaniem będzie utworzenie dwóch lokalnych grup bezpieczeństwa dla administratorów i użytkowników DHCP. Należy kliknąć w przycisk Wykonaj (Commit).



Następnie trzeba podać dane użytkownika, który ma uprawnienia niezbędne do autoryzacji serwera DHCP w usłudze Active Directory (Use the following user's credentials). Można także pominąć autoryzację (Skip AD authorization).

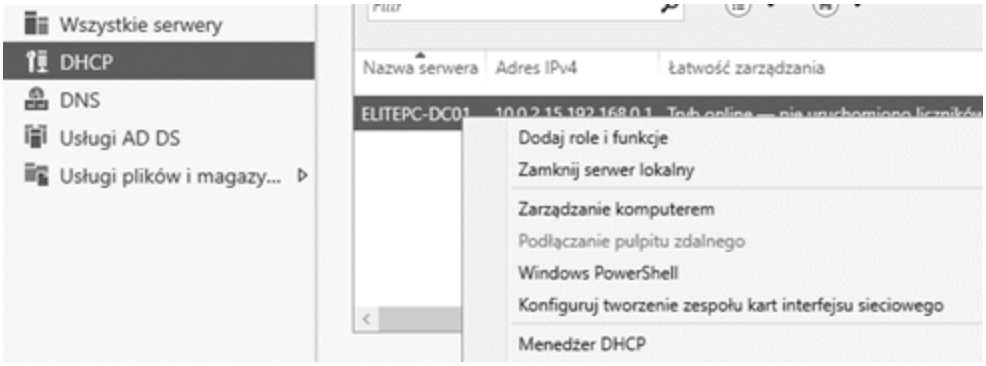


Wybór należy zaakceptować, a następnie zamknąć okno podsumowujące.

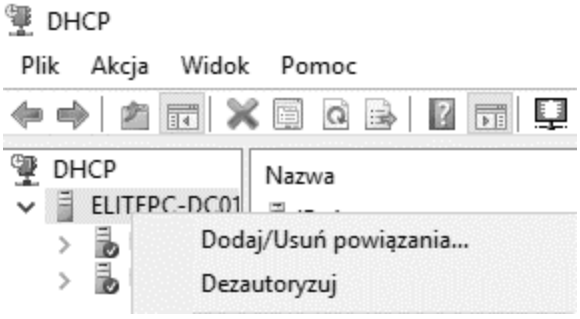


5.2. Konfiguracja serwera DHCP

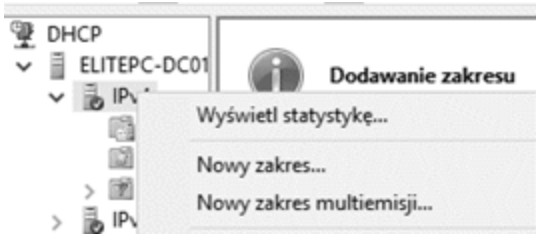
Kolejnym krokiem będzie wybranie DHCP w menu Menadżera serwera (Server Manager) znajdującym się z lewej strony, a następnym kliknięcie prawym przyciskiem myszy w wybrany serwer i wybranie opcji zarządzania nim Menadżer DHCP (DHCP Manager).



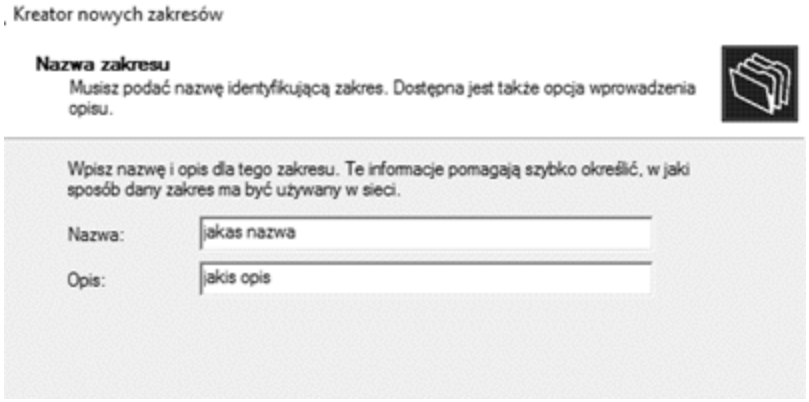
Jeżeli serwer nie został jeszcze autoryzowany w Active Directory, wystarczy kliknąć w niego prawym przyciskiem myszy i wybrać opcję Autoryzuj (Authorize). Jeżeli natomiast jest już autoryzowany, można ten krok pominąć. Jeśli AD i DHCP są instalowane na tej samej maszynie, serwer autoryzuje się sam – automatycznie.



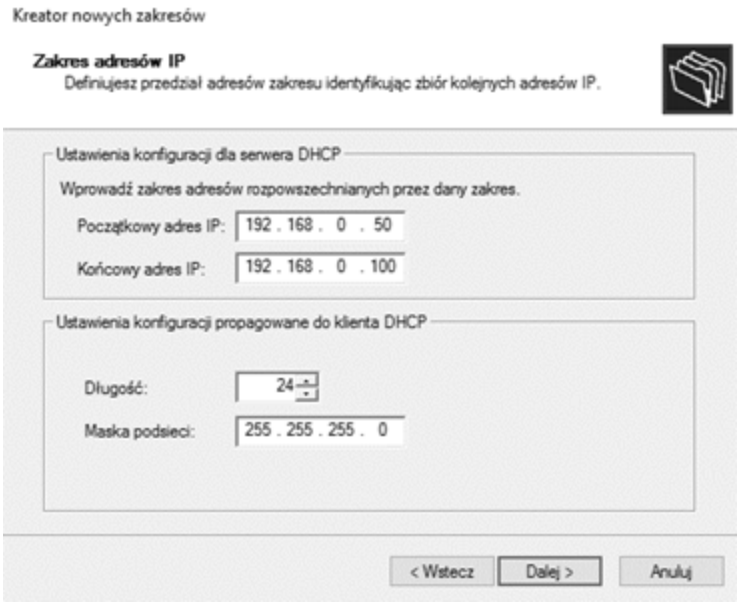
Kolejnym krokiem konfiguracji będzie stworzenie zakresów DHCP. Przykładowo, niech będzie stworzony taki zakres dla protokołu IPv4. W tym celu należy rozwinąć drzewo serwera i klikając prawym przyciskiem myszy na IPv4, wybrać opcję Nowy Zakres (New Scope).



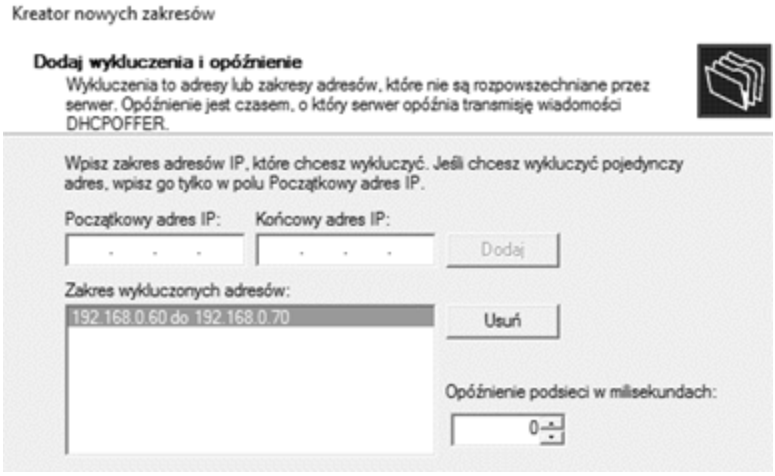
W pierwszej karcie kreatora podaje się Nazwę dla zakresu (Name) oraz Opis (Description), który będzie informował, za co zakres odpowiada.



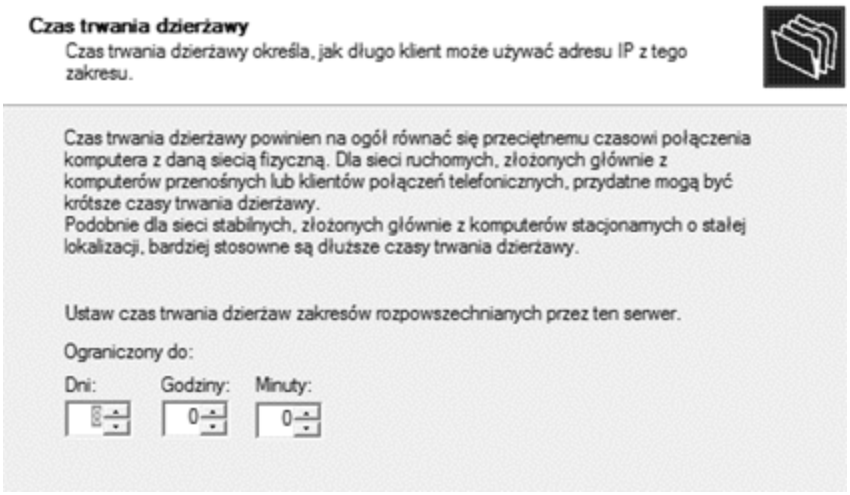
Na kolejnej karcie definiuje się dwa adresy IP. Jednym z nich będzie Początkowy adres IP (Start IP address), od którego DHCP zacznie przydzielać klientom adresy IP, a drugi to Końcowy adres IP (End IP address), na którym serwer zakończy ich przydzielanie. Należy podać także Maskę podsieci (Subnet Mask), która ma być przypisywana klientom.



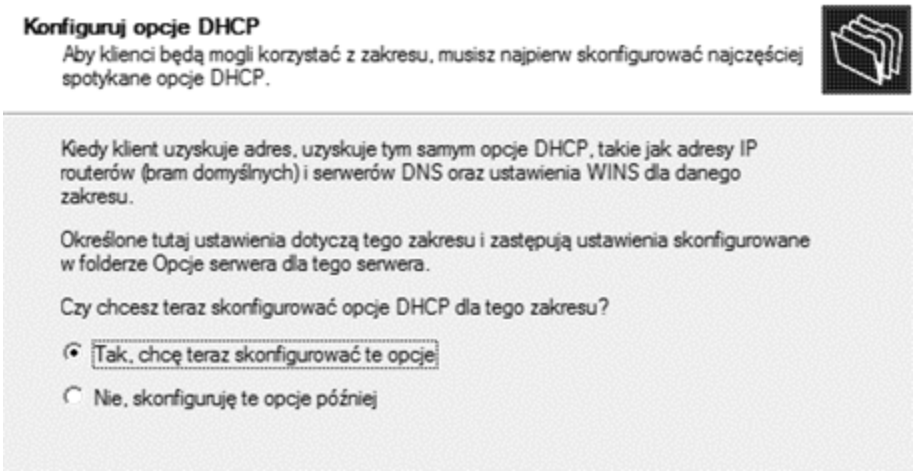
W kolejnym oknie analogicznie definiuje się zakres adresów IP z tym, że tym razem będą one dotyczyły puli adresów, które mają zostać wykluczone z wcześniej zdefiniowanej puli.



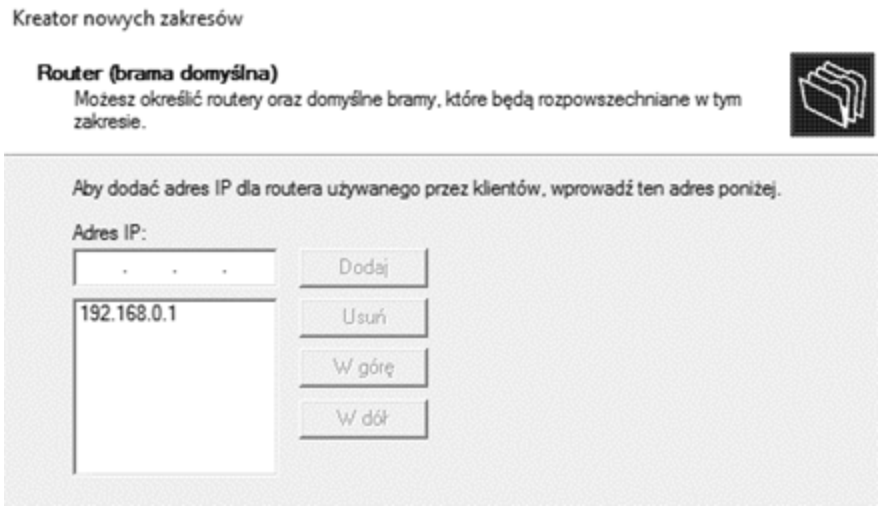
W kolejnym kroku należy określić, jak długo może trwać dzierżawa adresu. Domyślnie jest to osiem dni, po czym przydzielony adres jest zwalniany na potrzeby innego komputera.



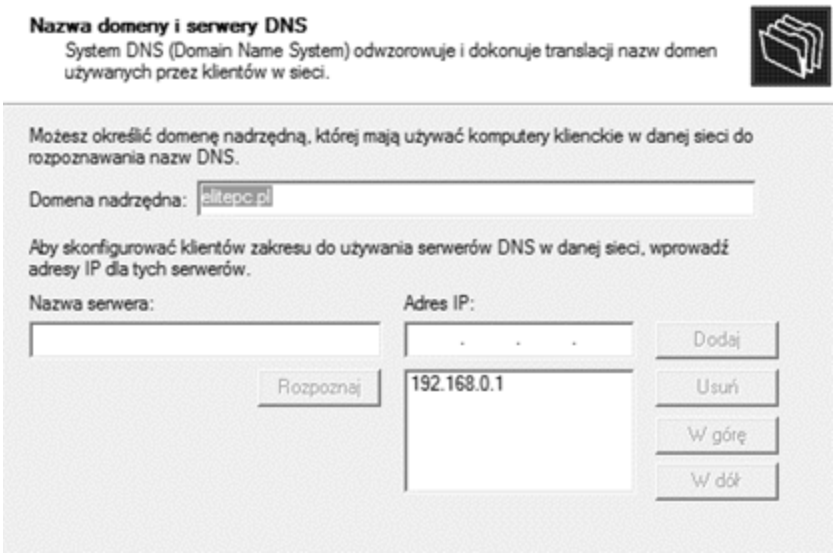
Można także skonfigurować opcje serwera DHCP. Na ogół ich konfiguracja jest zbędna do prawidłowego działania sieci. Dlatego też zostanie zaznaczona opcja pierwsza: Tak, chcę skonfigurować tę opcje teraz (Yes, I want to Configure these options now) – po to, by je od razu skonfigurować z poziomu kreatora.



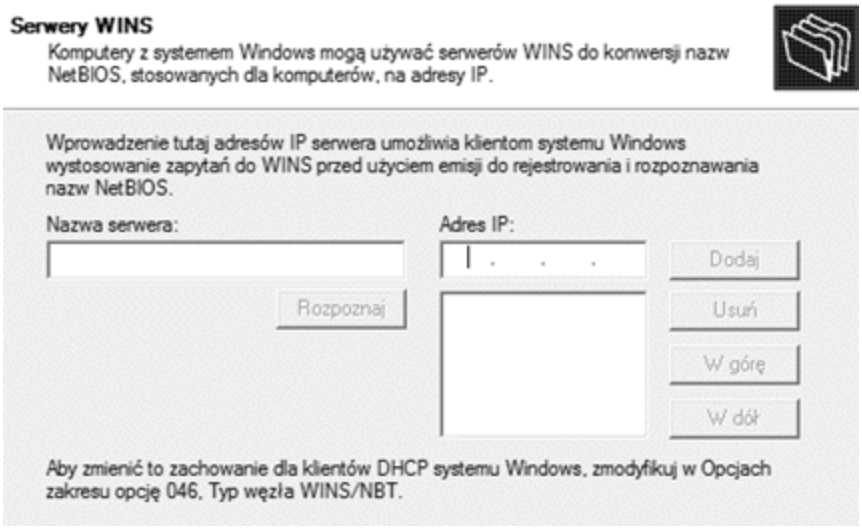
Jedną z nich będzie konfiguracja Routera (Bramki) (Router [Default Gateway]), gdzie wpisuje się adresy IP, pod którymi znajduje się wyjście z sieci na „świat”, np. Internet.



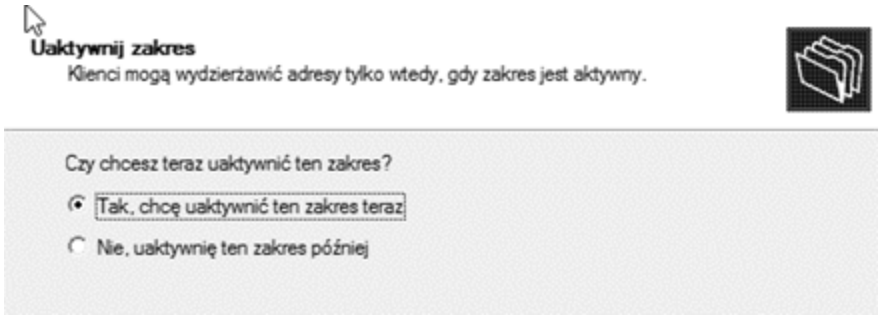
Następnie określa się adresy serwerów DNS, z jakich ma się korzystać w sieci i opcjonalnie nazwę domeny. Należy pamiętać, że jeśli maszyny mają prawidłowo pracować w domenie, niezbędne jest podanie wewnętrznych, firmowych adresów serwerów DNS, powiązanych z Active Directory.



Jeżeli korzysta się z serwerów WINS, w tym kreatorze także można określić ich sieciowe lokalizacje.



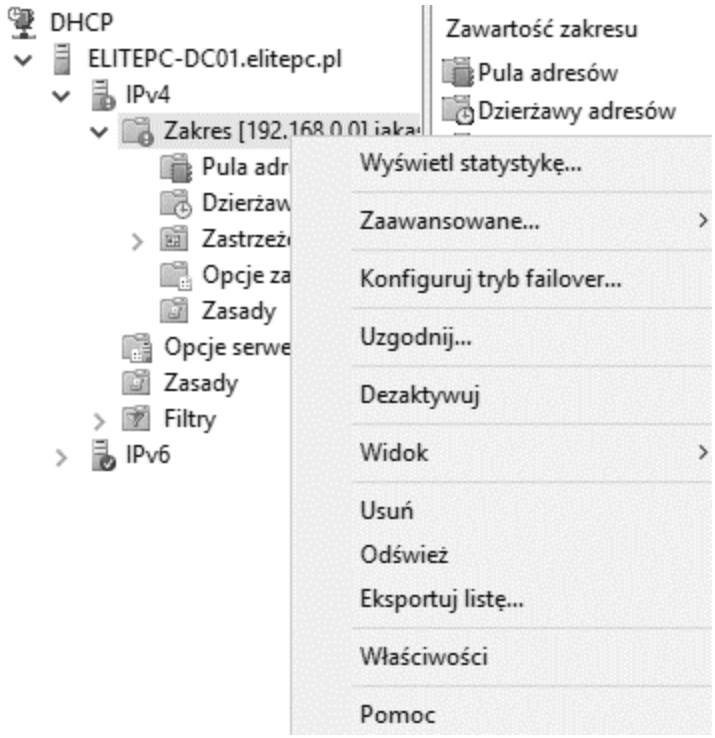
Ostatnim pytaniem, na jakie należy odpowiedzieć, jest to, czy kreator ma uruchomić stworzony zakres, czy też nie. Jeśli ma zostać uruchomiony, należy wybrać, że się chce (Yes, I want to deactivate this scope now).



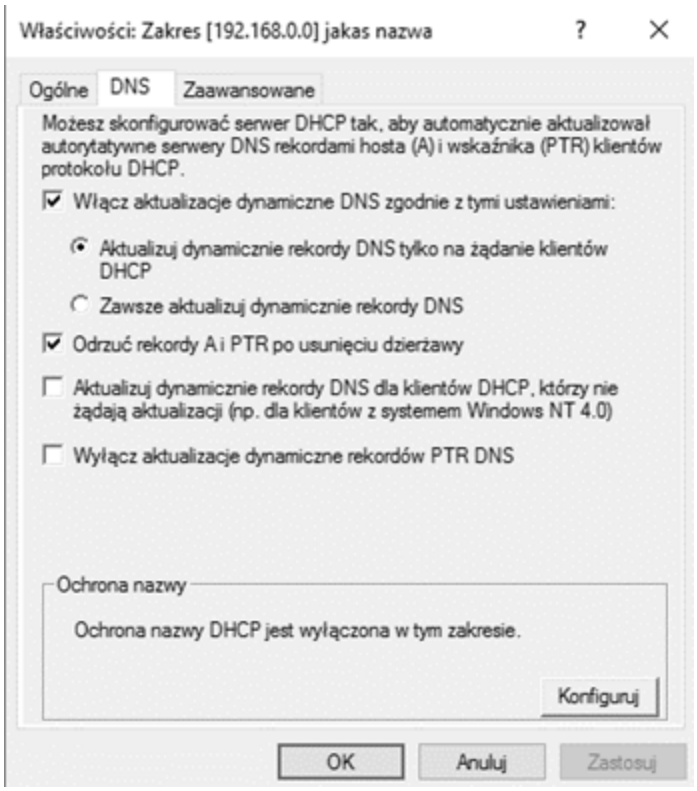
Przycisk Zakończ (Finish) zamyka kreatora.

5.3. Zarządzanie serwerem DHCP

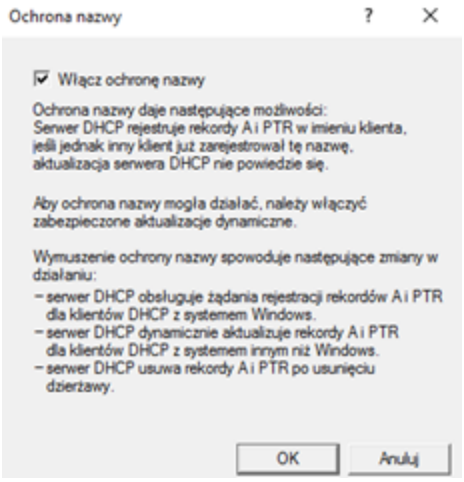
Po chwili serwer powinien być gotowy do pracy. Obok jego ikonki winna pojawić się zielona tarcza. Jeżeli nie pojawia się ona od razu, należy chwilę poczekać i odświeżyć widok (opcja w menu kontekstowym, bądź guzik F5 na klawiaturze). Stworzony zakres można zawsze skasować, klikając w niego prawym przyciskiem myszy i wybierając Usuń (Delete). Mniej inwazyjną metodą jego wyłączenia będzie Dezaktywacja (Deactivate).



W ramach zakresu można między innymi wejść w jego Właściwości (Properties). Znajdują się tam dodatkowe możliwości konfiguracyjne. We właściwościach znajduje się zakładka DNS, gdzie można skonfigurować pozostałe opcje związane z aktualizacjami dynamicznymi. Jest to krok niezbędny, aby dynamiczne aktualizacje działały. Trzeba więc zapamiętać, że ich konfiguracja jest dwustopniowa. Należy je uruchomić zarówno po stronie serwera DNS jak i serwera DHCP.

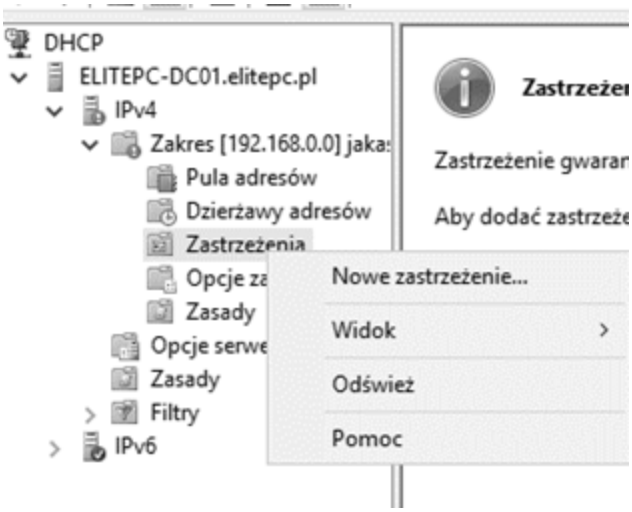


W sekcji Ochrona nazwy (Name Protection) można kliknąć w przycisk Konfiguruj (Configure) i uruchomić ochronę, która sprawi, że duplikaty rekordów DNS nie wystąpią.

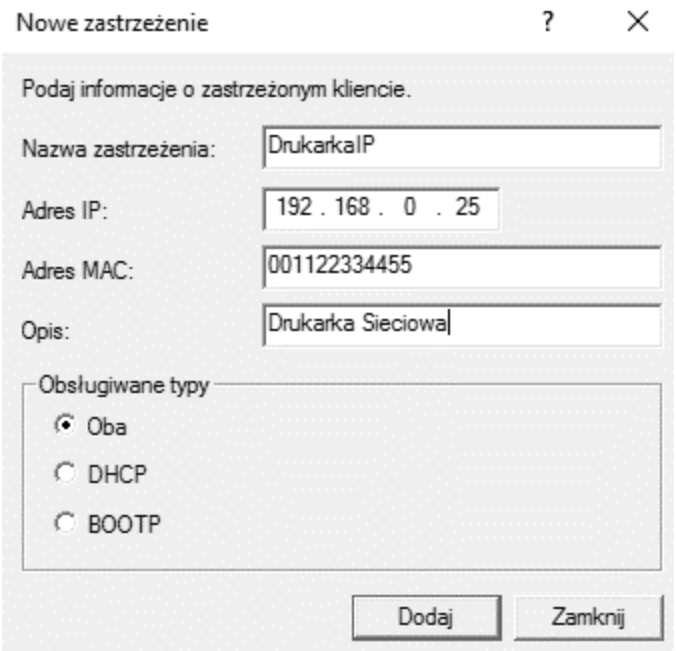


W łatwy sposób można także stworzyć zastrzeżenie, które będzie bardzo przydatne, kiedy dany adres IP ma być zarezerwowany dla drukarki czy innego komputera. Zawsze będzie on miał przypisany konkretny adres. Wystarczy

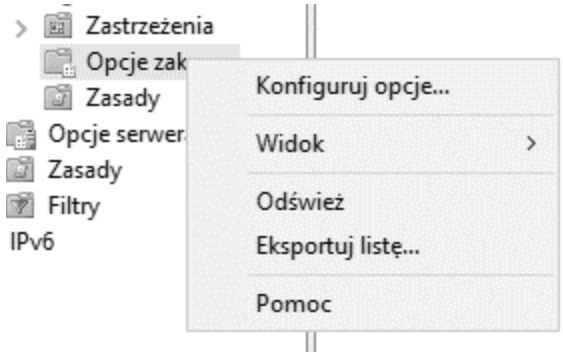
w Rezerwacje (Reservations) kliknąć prawym przyciskiem myszy i wybrać Nowe zastrzeżenie (New Reservation).



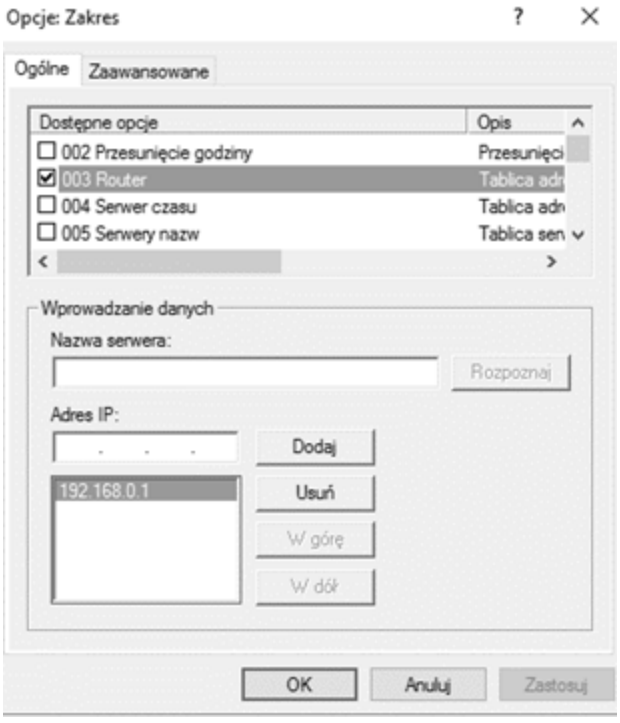
Pojawi się małe okienko, w którym należy podać Nazwę zastrzeżenia (Reservation Name), adres IP (IP address), który ma być przypisany temu urządzeniu, a także Adres MAC (MAC address) karty sieciowej tego urządzenia, dzięki czemu serwer DHCP je rozpozna w sieci. Można także wprowadzić Opis (Description).



Bardzo pożyteczne i przydatne są opcje zakresu. Trzy z nich zostały już skonfigurowane, lecz czasami może się to okazać niewystarczające. Należy więc kliknąć prawym klawiszem myszy w Opcje zakresu (Scope Options) i wybrać Konfiguruj opcje (Configure Options).

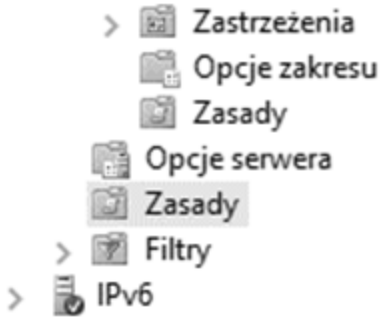


To właśnie w nich definiuje się adres IP routera, serwera czasu czy serwera PXE. Ustawienia te często są bardzo przydatne, a nierzadko niezbędne.

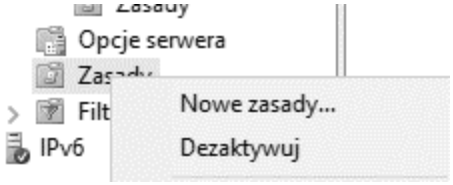


5.3.1. DHCP Policies

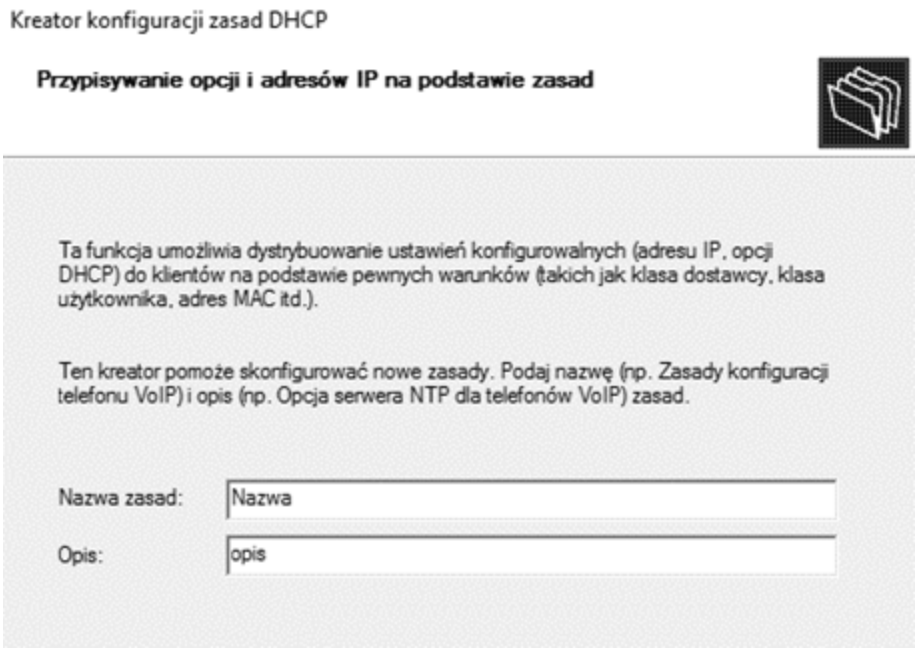
Omówione do tej pory moduły serwera DHCP nie uległy zmianie względem starszych wersji sytemu Windows Server. W wersji 2016 pojawiły się jednak Polityki (Policies). Warto zauważyć, że można je definiować na poziomie serwera (dla wszystkich zakresów) lub na poziomie jedynie wybranego zakresu. Na rysunku poniżej występują one w dwóch miejscach.



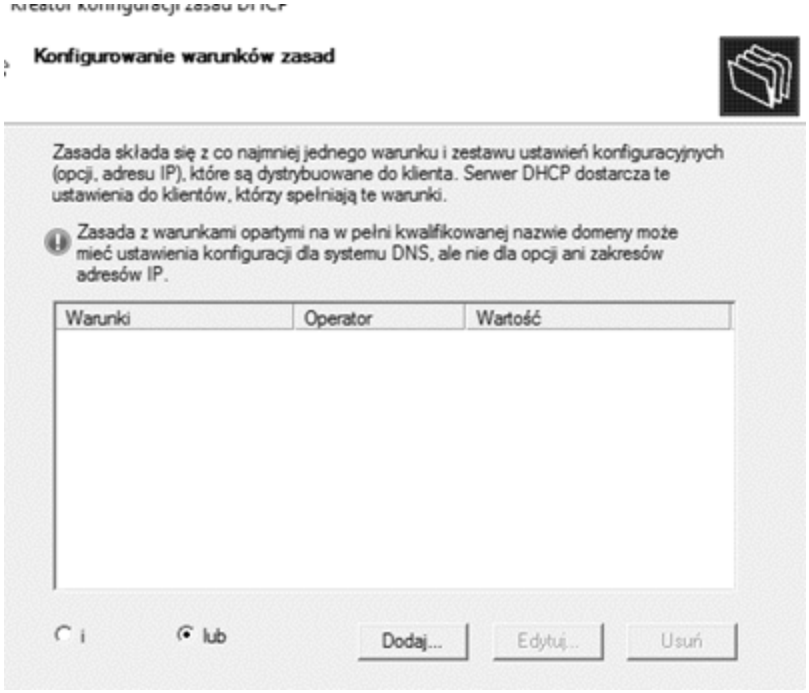
Polityki pozwalają na określenie zasad przydzielania adresów urządzeniom, które, aby dostać adres IP, będą musiały spełniać pewne predefiniowane kryteria. Aby takie kryterium określić Należy kliknąć na Polityki (Policies) prawym przyciskiem myszy i wybrać Nowa Polityka (New policy).



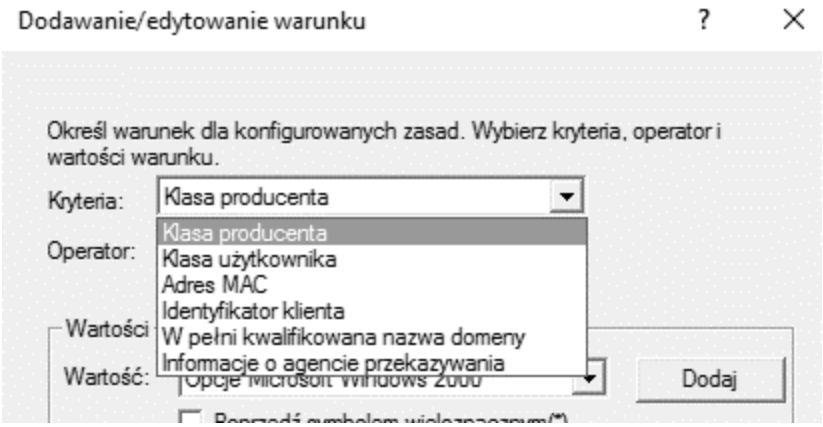
W pierwszym oknie kreatora konieczne jest podanie nazwy oraz opisu polityki.



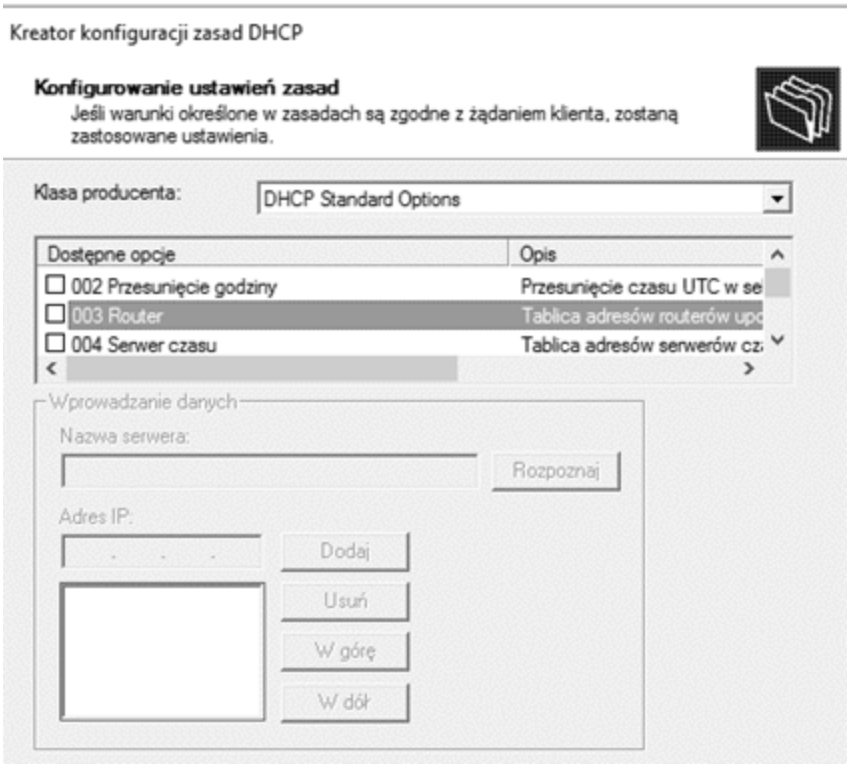
W następnym oknie kreatora definiuje się kryteria, jakie dane urządzenie musi spełnić. Kryteriów może być kilka i mogą być połączone operatorem logicznym AND (urządzenie musi spełniać wszystkie kryteria) lub OR (urządzenie musi spełniać minimum jedno kryterium). Kryteria dodaje się przyciskiem ADD.



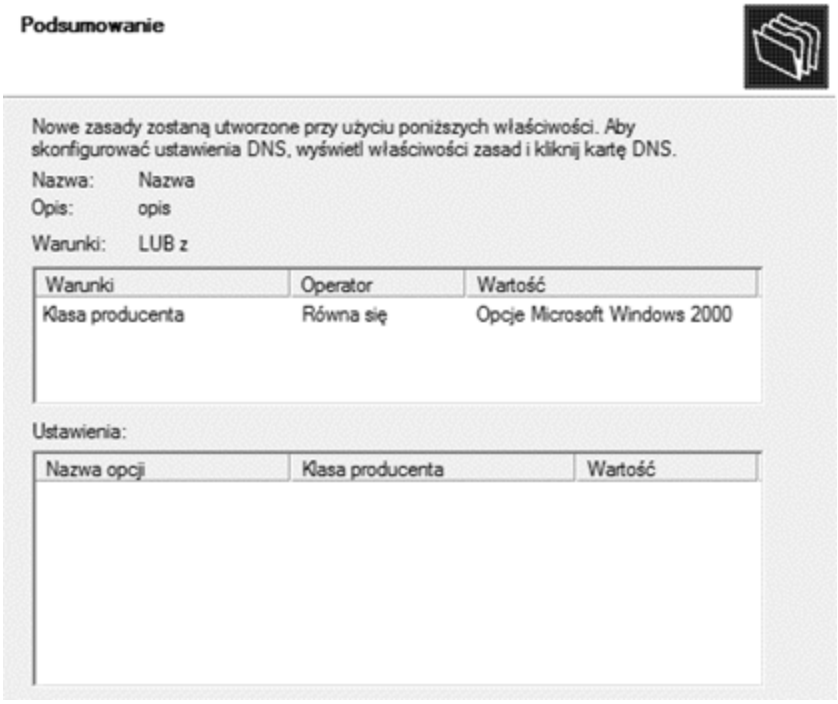
Następnie należy określić kryterium warunku, jest które ma kilka klas. Jedną z nich jest Vendor Class, która pozwoli określić dolną granicę wersji sytemu Windows, User, która pozwala udzielać dostępu na podstawie uprawnień użytkowników, MAC, która pozwala na filtrowanie według adresów MAC oraz Client Indetifier i Relay Agent Information.



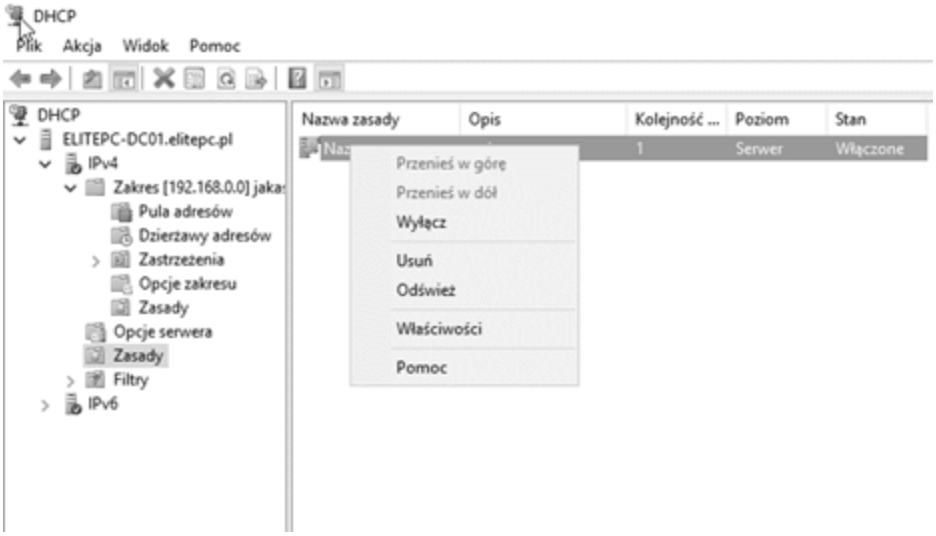
Należy kliknąć OK, aby powrócić do kreatora, a następnie kliknąć Dalej (Next). Włączy się karta konfiguracji opcji serwera. W dalszej kolejności należy zdefiniować, jakie opcje zostaną przypisane klientom, których obejmie kryterium. Można więc mieć inne opcje dla maszyn spełniających kryteria i dla tych, które ich nie spełniają.



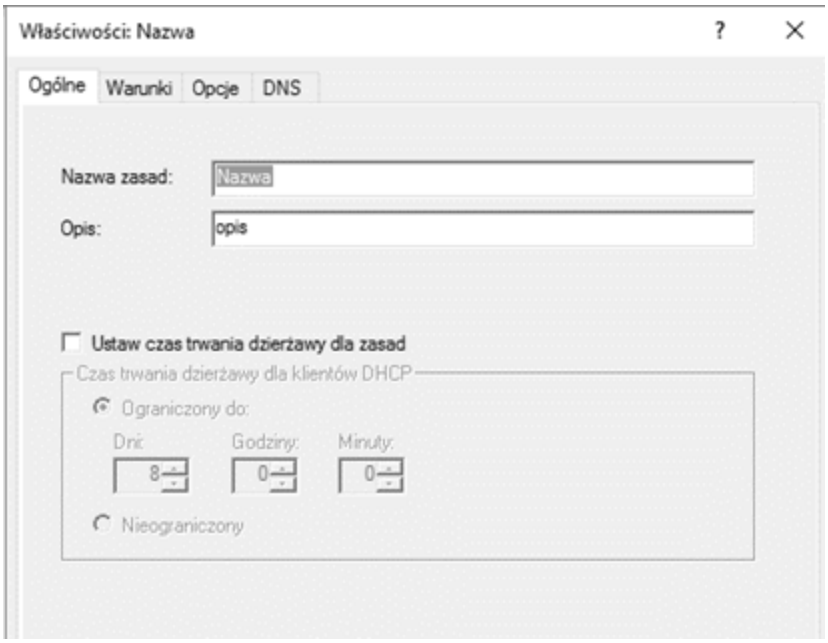
Na karcie podsumowującej należy kliknąć Zakończ (Finish).



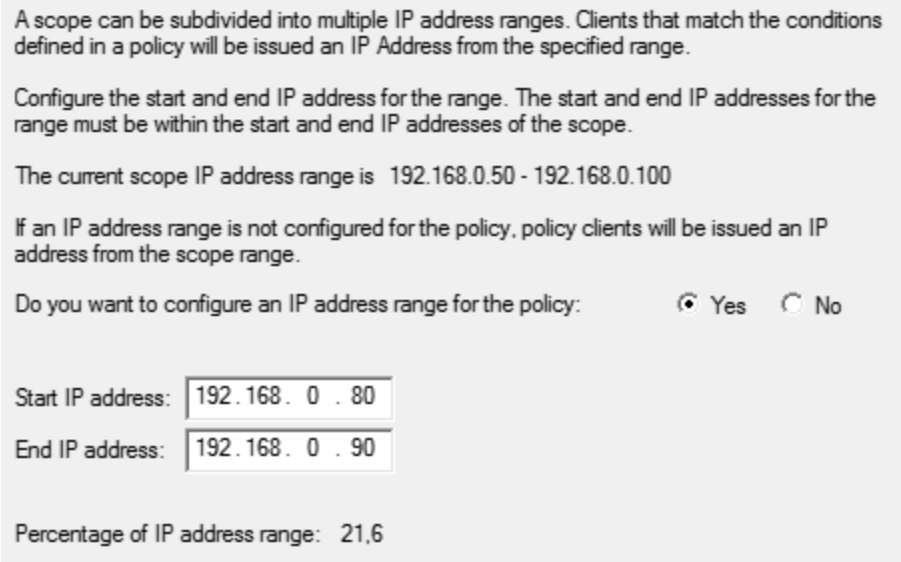
Utworzona polityka zostanie wyświetlona na liście. Po kliknięciu na niej prawym klawiszem myszy, w menu kontekstowym pokażą się opcje pozwalające ją Wyłączyć (Disable), Skasować (Delete), Przenieść w górę (Move Up) lub Przenieść w dół (Move Down), aby określić jej ważność. Im polityka znajduje się wyżej na liście, tym jest ważniejsza.



Wchodząc we Właściwości (Properties) danej polityki, można je modyfikować.



W przypadku polityki tworzonej po zmianie konkretnego zakresu, w kreatorze pojawi się jeszcze jedna karta, która pozwala na stworzenie podzakresu adresów IP dla urządzeń, które są objęte daną polityką. „Mini” zakres musi znajdować się wewnątrz zakresu ogólnego.



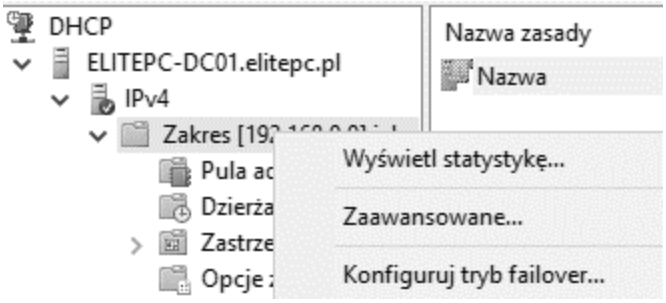
5.4. Wysoka dostępność DHCP

Każdy serwer, w tym także DHCP, musi być dostępny 24 godziny na dobę, 7 dni w tygodniu. Nawet podczas awarii serwera firma powinna móc dalej funkcjonować, jak gdyby nic się nie stało z punktu widzenia użytkowników. Dlatego też tworzy się serwery zapasowe, które przejmują role głównych maszyn w razie ich awarii, przeciążenia lub niedostępności z innych powodów. Serwery te duplikują

także dane. Za chwilę czytelnik dowie się jak zapewnić ciągłość i bezpieczeństwo działania serwera DHCP.

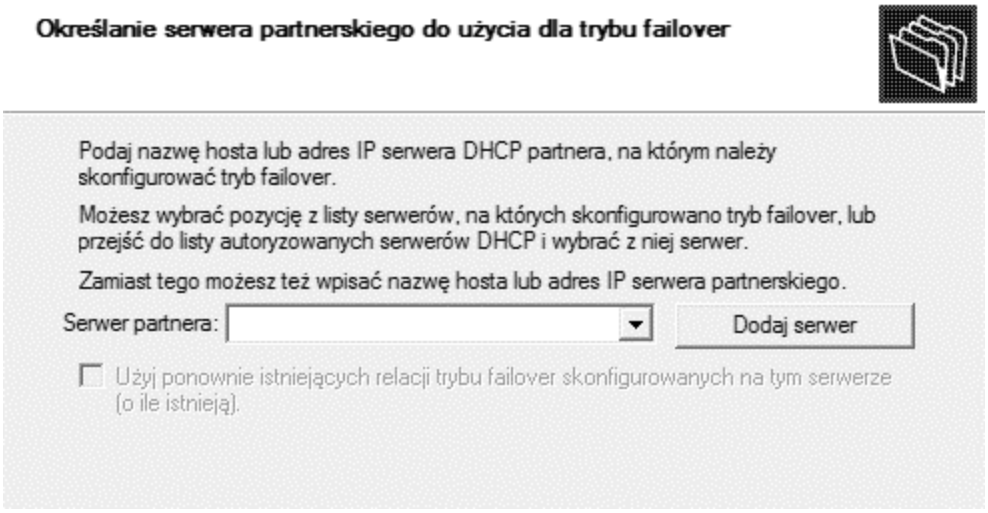
5.4.1. Konfiguracja klastra DHCP

Nowością w serwerze DHCP są elementy wysokiej dostępności związane z klastrami. Zostały one oparte na IETF-DHCP Failover Protocol. Przed kontynuacją należy pamiętać, że klaster wymaga systemu Windows Server w wersji Datacenter. Podobnie jak polityki, klastry można definiować dla zakresów jak i dla całego serwera. Pamiętać należy także o tym, aby w serwerze DHCP istniał przynajmniej jeden zakres. Jeżeli go nie będzie, kreator konfiguracji nie pozwoli przejść do kolejnego kroku. Rzeczą naturalną jest to, że w sieci musi istnieć drugi server DHCP pod kontrolą Windows Server 2016, dlatego też dla utworzonego zakresu zostanie stworzony klaster. W tym celu należy kliknąć na zakresie prawym przyciskiem myszy i wybrać Konfiguruj klaster (Configure Failover).

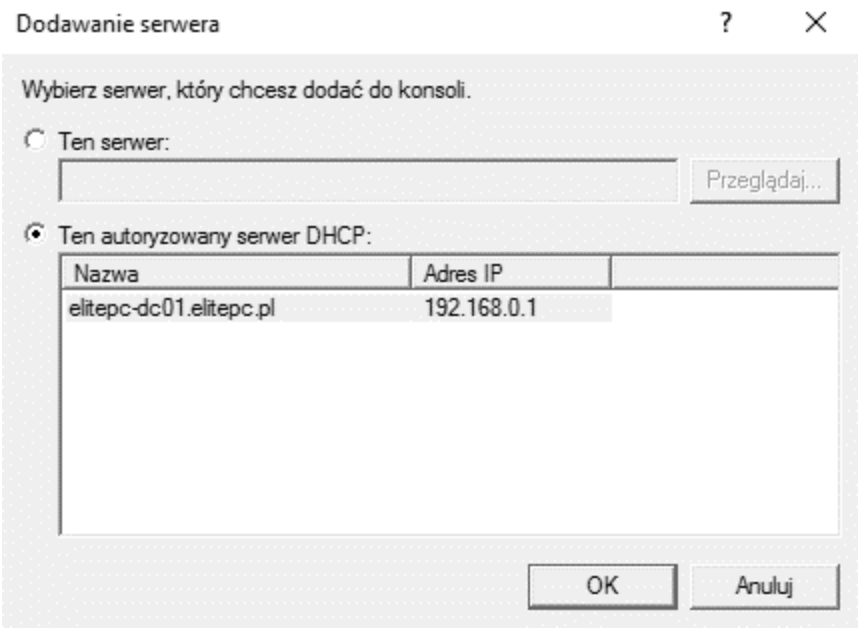


Na pierwszej karcie należy zdefiniować zakresy, które będą wykorzystywane, bądź zaznaczyć opcję Zaznacz Wszystko (Select All), aby wybrać wszystkie dostępne zakresy. Należy kliknąć przycisk Dalej (Next).

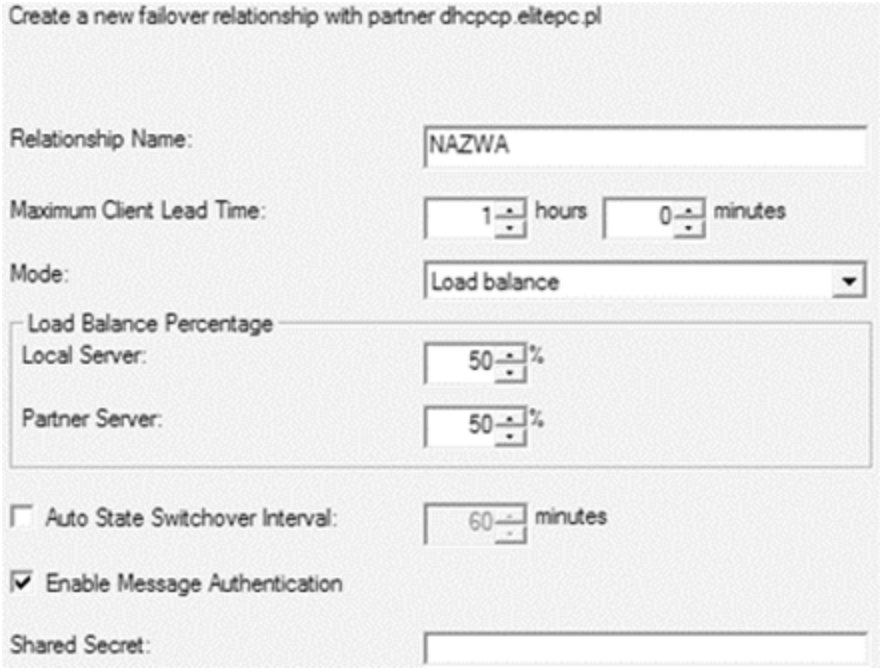
W kolejnym oknie konieczne jest wskazanie serwera partnerskiego, na którym replika będzie przechowywana. Będzie nią nie tylko baza danych DHCP, ale i konfiguracja serwera.



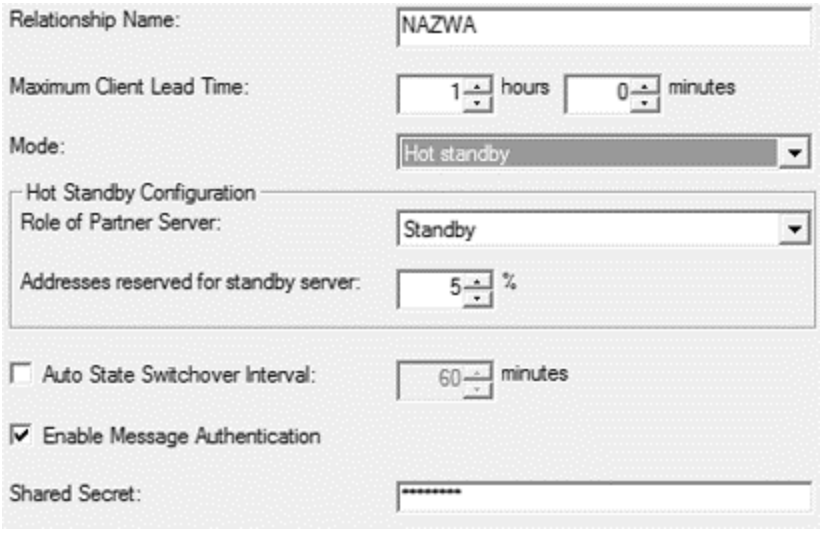
Przyciskiem Dodaj Serwer (Add Server) należy go wybrać. Serwer musi już być autoryzowany w domenie. Dla jednego zakresu można wybrać tylko jeden serwer partnerski.



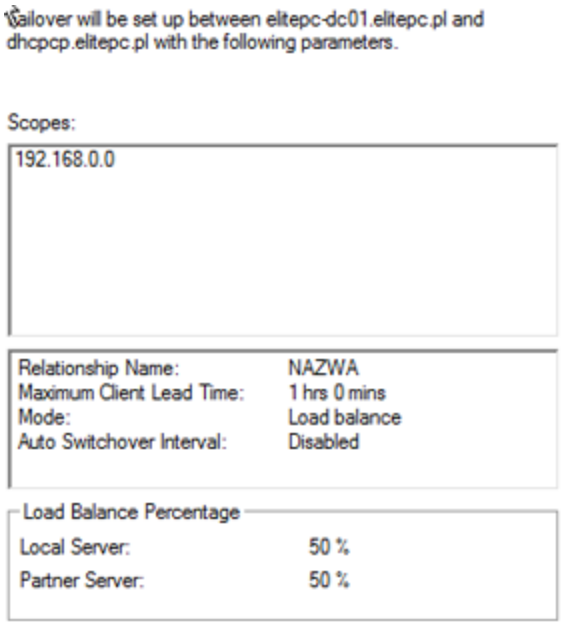
W kolejnym oknie relacji pomiędzy serwerami należy nadać nazwę. Wybiera się tu także Tryb działania relacji (Mode). Do wyboru jest Zrównoważenie Obciążenia (Load Balance), który będzie w określonym procentowo stopniu równoważył obciążenie serwera DHCP. Warto także ustawić czas w opcji Maximum Client Lead Time, informującej o tym, jak długo trwa czas dzierżawy dla klienta, który dostał dzierżawę adresu IP z dowolnego z serwerów. Jest on ważniejszy od czasu dzierżawy określonego dla zakresu. Warto także wybrać Enable Message Authentication i wprowadzić hasło o wysokiej złożoności. Dzięki temu komunikacja pomiędzy serwerami będzie szyfrowana funkcją SHA-2.



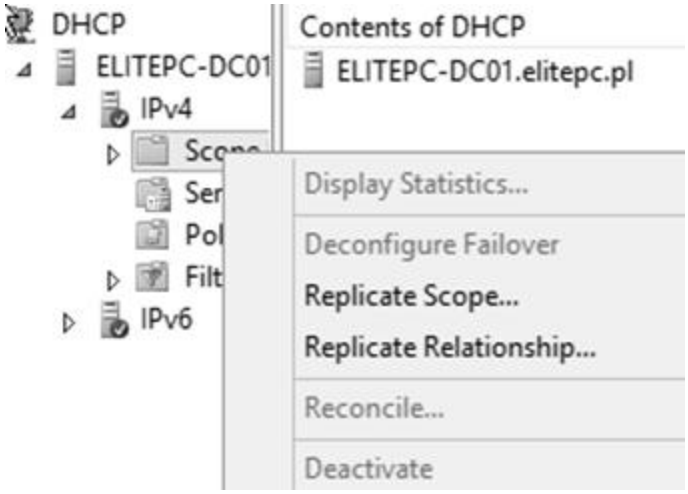
Drugim trybem pracy jest Hot Standby. Tworzy on replikę, która przejmie rolę głównego serwera DHCP w razie jakichś problemów z dostępnością serwera głównego. Warto w nim użyć opcji Auto State Switchover Interval, określającej, po jakim czasie od braku komunikacji z serwerem głównym zapasowy przejmie jego funkcje.



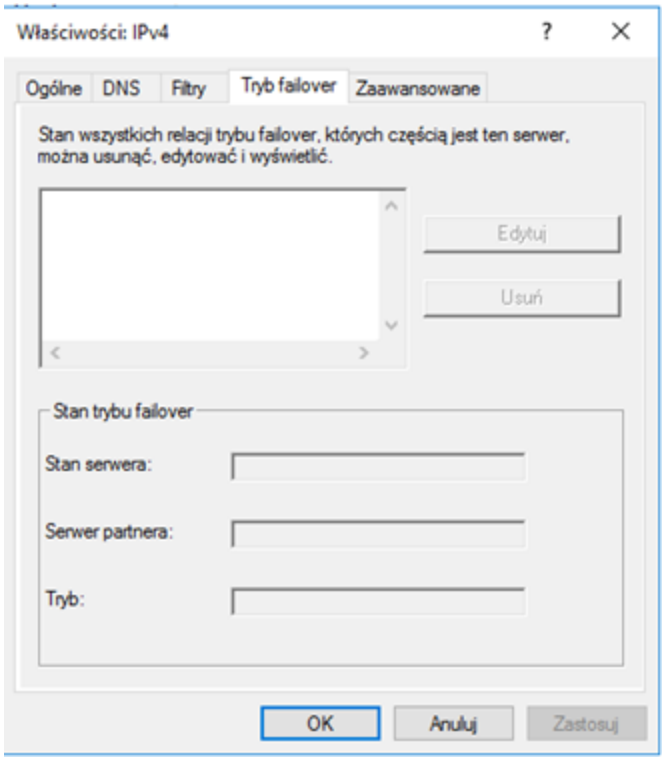
Kolejna karta to podsumowanie, na której należy kliknąć Zakończ (Finish).



Teraz dla zakresów pod prawym przyciskiem myszy dostępne będą dodatkowe funkcje związane z replikacją.

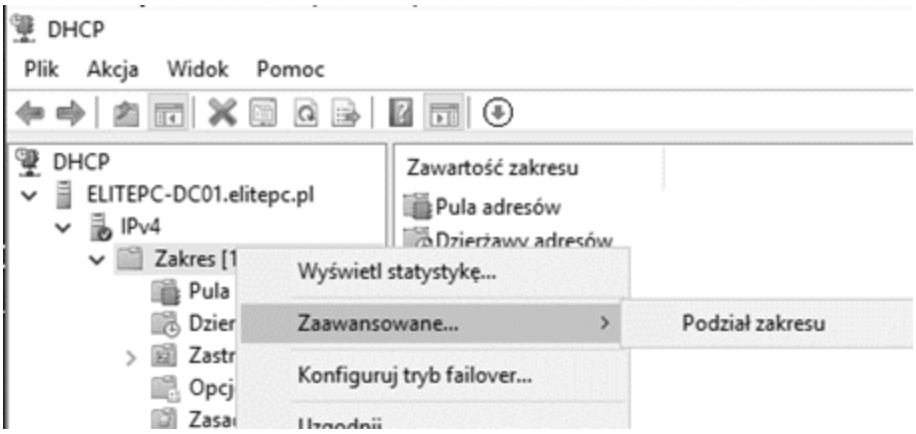


Aby skasować taką relację wystarczy wejść we właściwości IPv4, a następnie w zakładkę Failover.

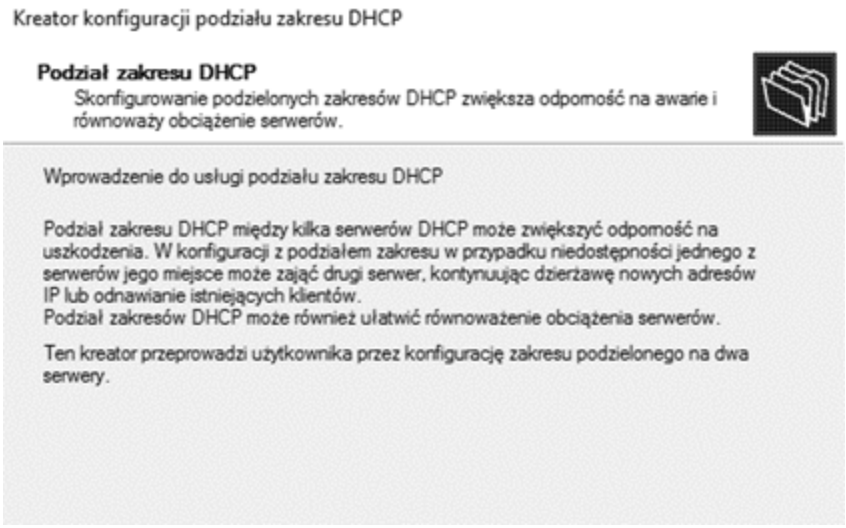


5.4.2. Split-Scope

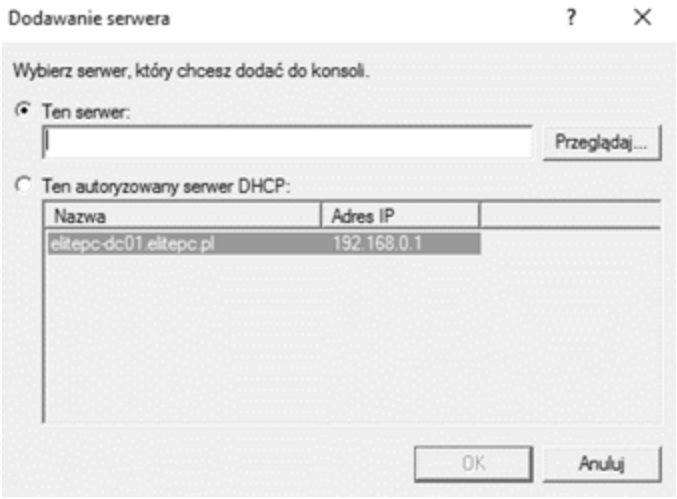
Jeżeli nie zostanie stworzony klaster ,można użyć funkcji znanej już z Windows Server 2008. Mowa tu o Split-Scope. Dzięki niej można stworzyć dwa serwery DHCP, pomiędzy którymi wybrany zakres zostanie rozdzielony, a w razie awarii serwera, drugi przejmie jego rolę do czasu, aż uszkodzony nie wróci do pełnej funkcjonalności. W tym celu wystarczy kliknąć prawym przyciskiem na pożądanym zakresie, rozwinąć Advanced (Zaawansowane) i wybrać Split-Scope.



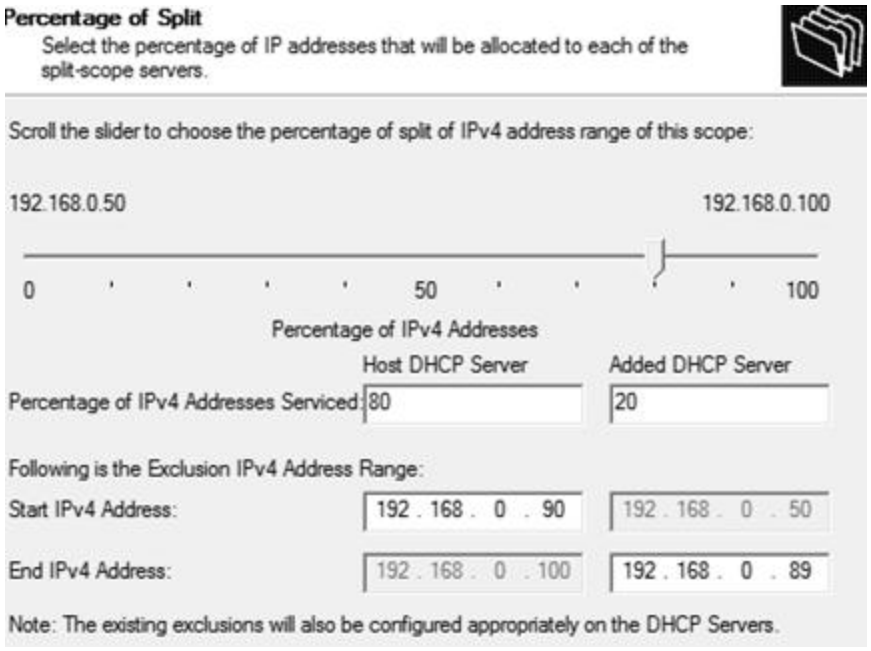
Na karcie powitalnej należy kliknąć Dalej (Next).



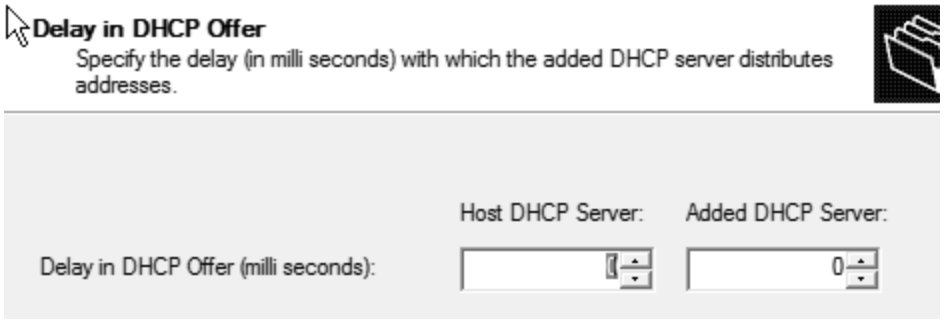
Następnie, podobnie jak w przypadku klastra, należy określić serwer zapasowy. Również musi być autoryzowany w AD.



W kolejnym oknie konieczne jest określenie w procentach, jaka część adresów będzie obsługiwana na głównym serwerze DHCP, a jaka na obecnie dodawanym (na zrzucie ekranu – 20%).



Następnie należy określić, po jakim czasie zapasowy DHCP ma przydzielić adres, czyli ile czasu na reakcję dostaje serwer podstawowy.



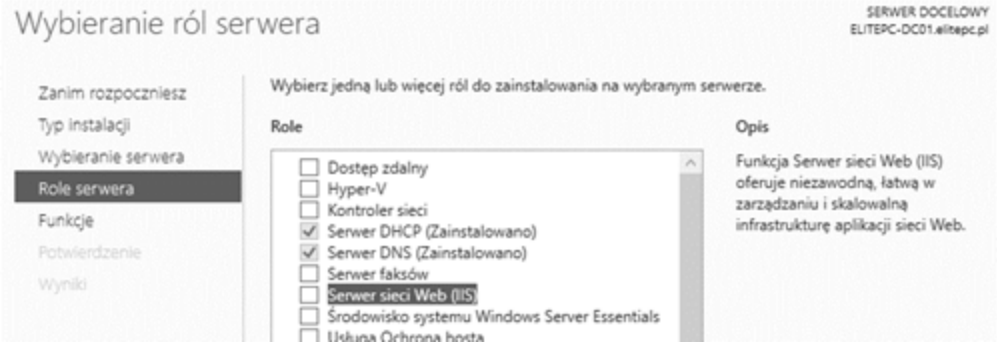
Na karcie podsumowującej należy kliknąć Zakończ (Finish).

6. IIS z FTP oraz Urząd Certyfikacji

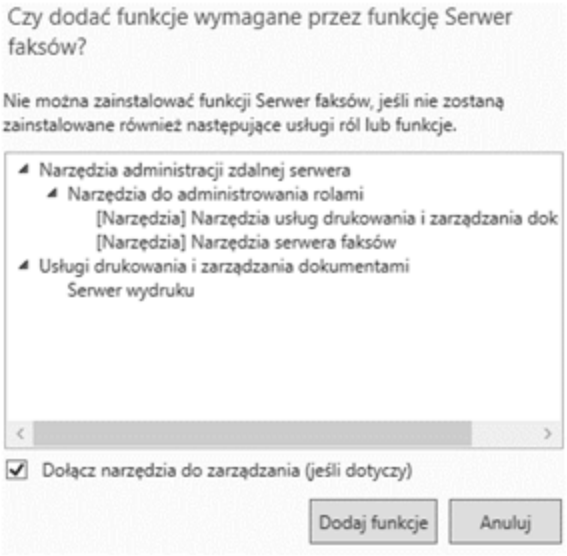
Internet Information Services to rola serwera, pozwalająca na hostowanie i publikowanie stron internetowych. Istnieje także możliwość publikacji witryn FTP. Obie te funkcje zostaną omówione w niniejszym rozdziale. Omówiony zostanie także Urząd Certyfikacji, ponieważ jego działanie i istnienie jest ściśle powiązane z serwerem www.

6.1. Instalacja roli Web Server (IIS)

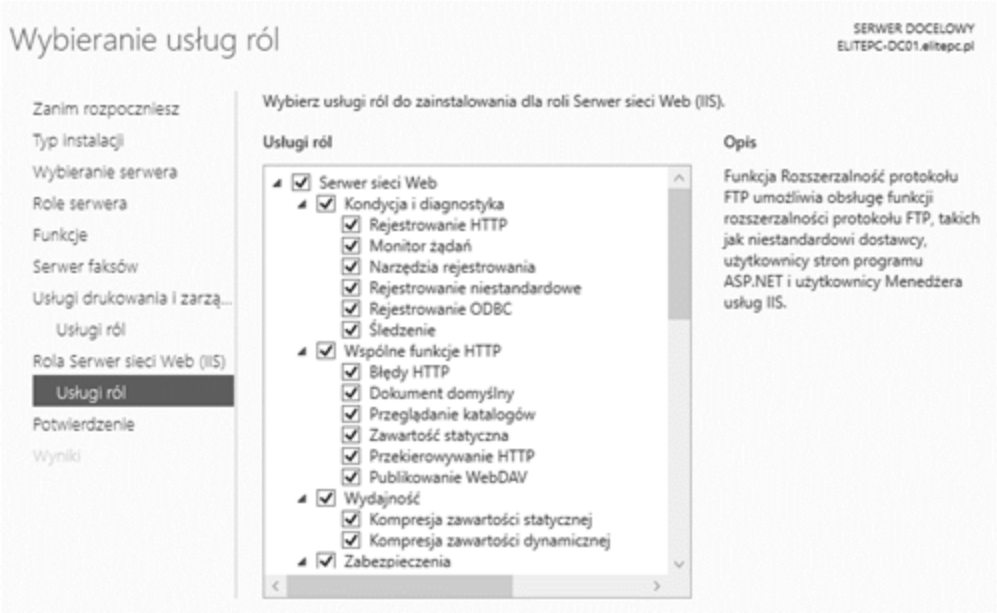
Na początku należy zainstalować rolę Web Server (IIS) przy pomocy Menadżera Serwera (Server Manager).



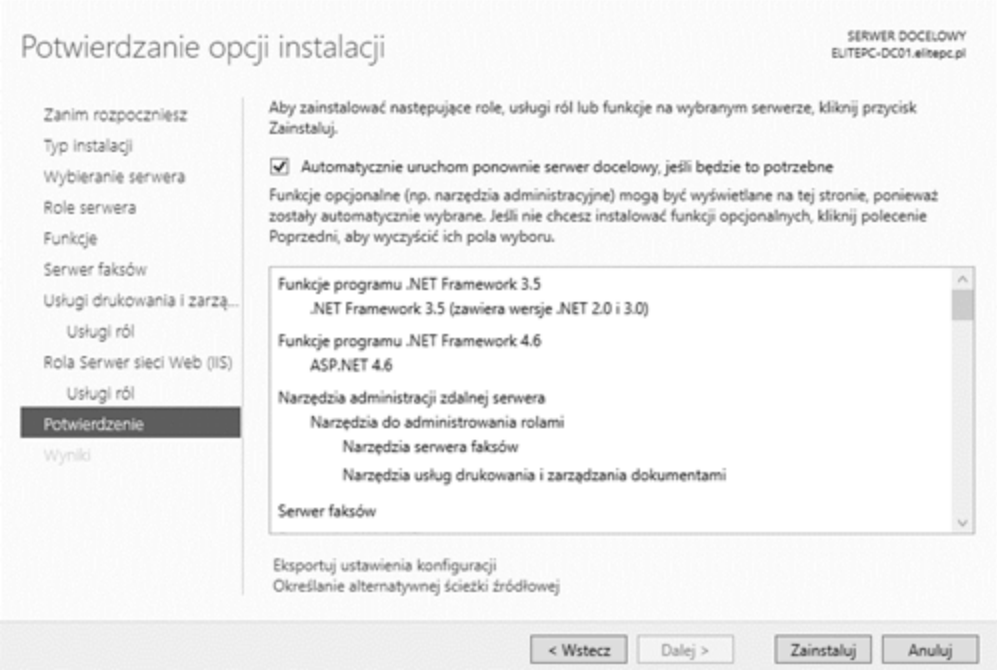
Należy zainstalować wymagane dodatki, a następnie zaakceptować je przyciskiem Dodaj funkcję (Add Features).



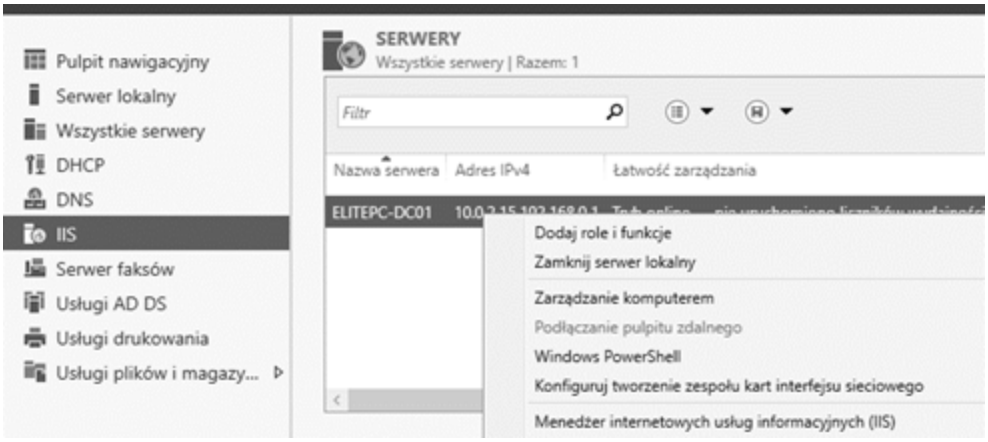
Spokojnie można zainstalować wszystkie usługi dostępne w serwerze IIS, aby w razie potrzeby nie musieć czegoś dodatkowo instalować. Można więc zaznaczyć wszystkie składniki IIS.



Proces instalacji tylu usług jednocześnie chwilę potrwa. Mimo że kreator tego nie wymaga, po instalacji warto uruchomić serwer ponownie.

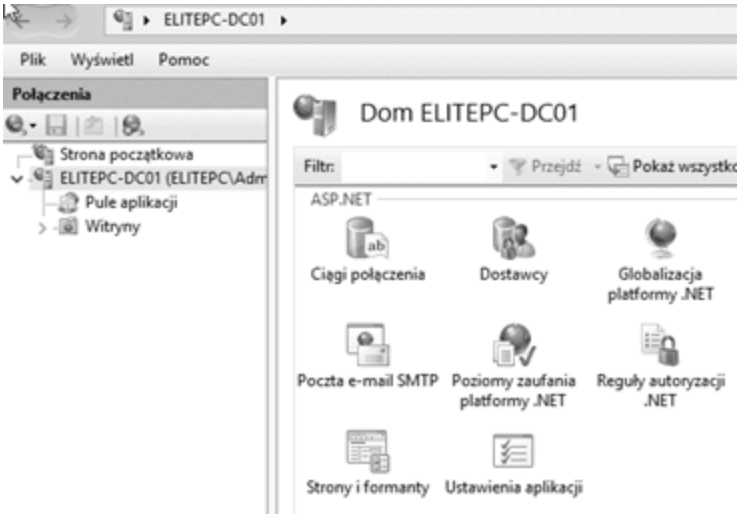


Menadżera IIS można odnaleźć w Menadżerze serwera (Server Manager) w menu po lewej stronie. Podobnie jak w przypadku innych ról, po kliknięciu na nim w centralnej części okna pojawi się lista serwerów, którymi można zarządzać. Po kliknięciu w wybrany prawym przyciskiem myszy, należy wybrać Menadżera IIS (Internet Information Services [IIS] Manager).



Standardowo uruchomiona jest już Domyślna Witryna. Najłatwiej jest wgrać swoją stronę www do katalogu

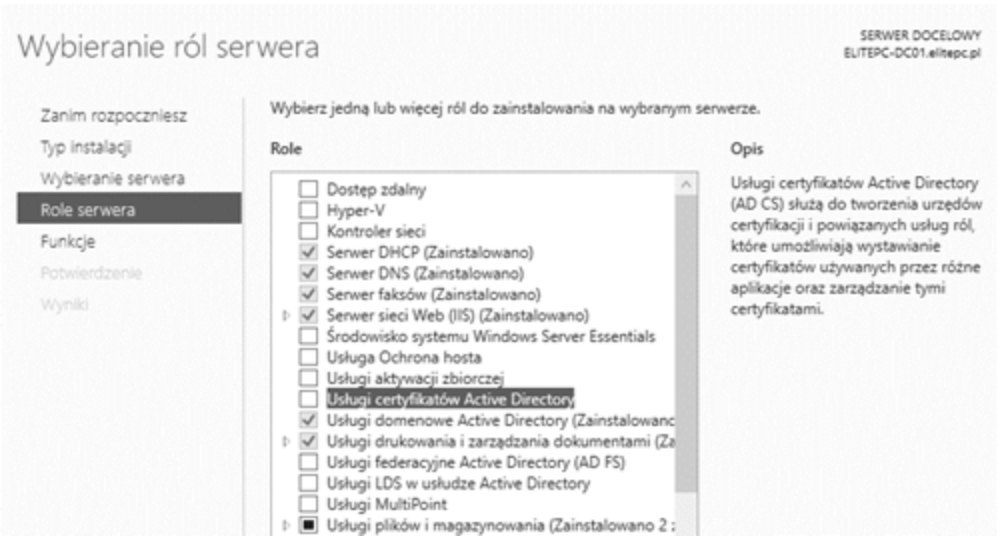
C:\inetpub\wwwroot, aby zadziałała poprawnie. Jej możliwości będą ograniczone do najbardziej elementarnych funkcjonalności, a także nie będzie ona w żaden sposób zabezpieczona, np. logowaniem. Co więcej, doświadczeni użytkownicy Windows Server zauważą, że z punktu widzenia interfejsu użytkownika nie widać na pierwszy rzut oka zmian względem serwera IIS w Windows Server 2008.



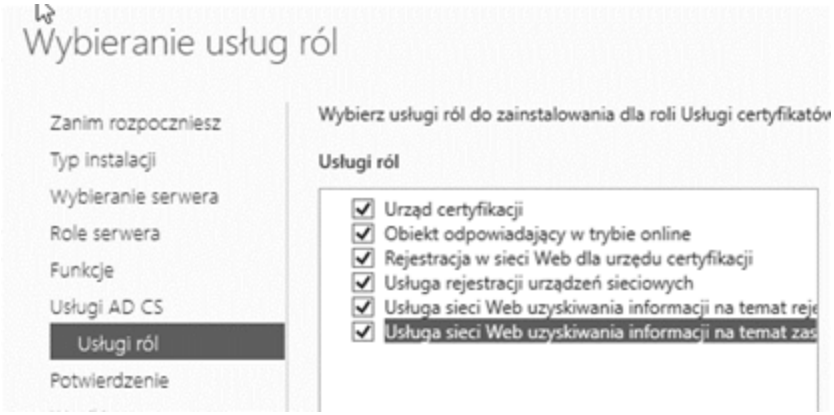
6.2. Instalacja Active Directory Certificate Services

Po instalacji serwera IIS warto zainstalować Urząd Certyfikacji (Certification Authority). IIS zawiera w sobie część składników wymaganych przez Urząd Certyfikacji (CA, od Certification Authority), a same certyfikaty przydadzą się między innymi do zabezpieczenia witryny www. Zostanie

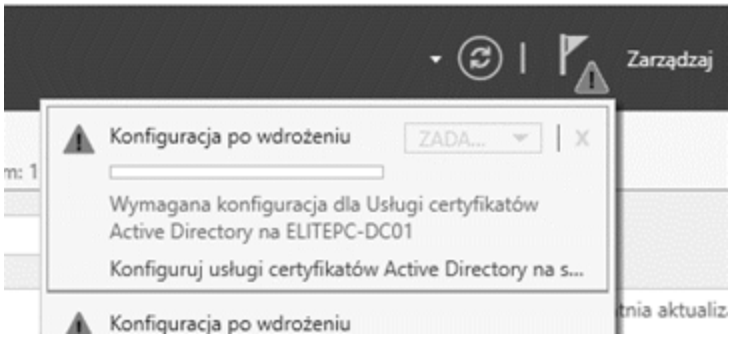
więc zainstalowana rola Active Directory Certificate Services wraz ze wszystkimi dodatkami.



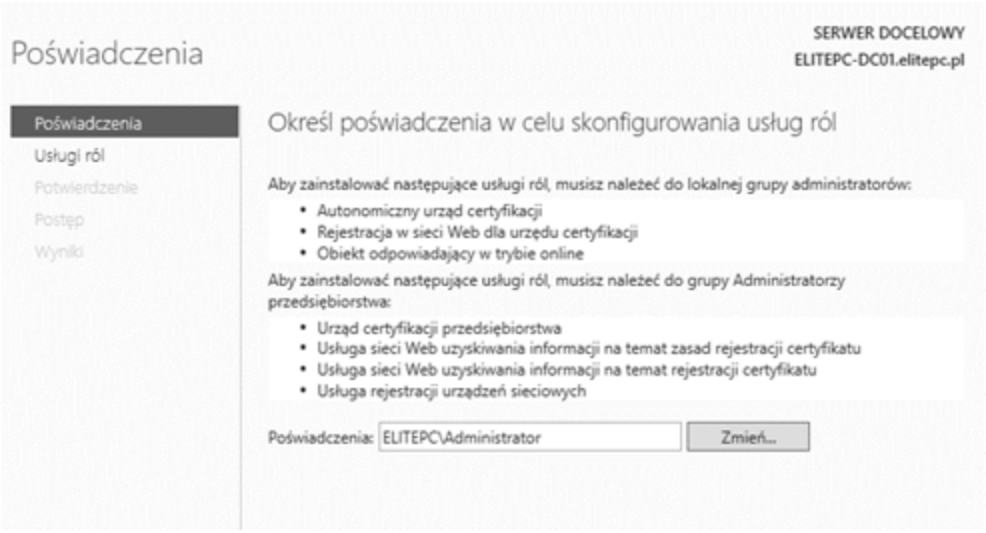
Należy wybrać Usługi Roli (Role Services).



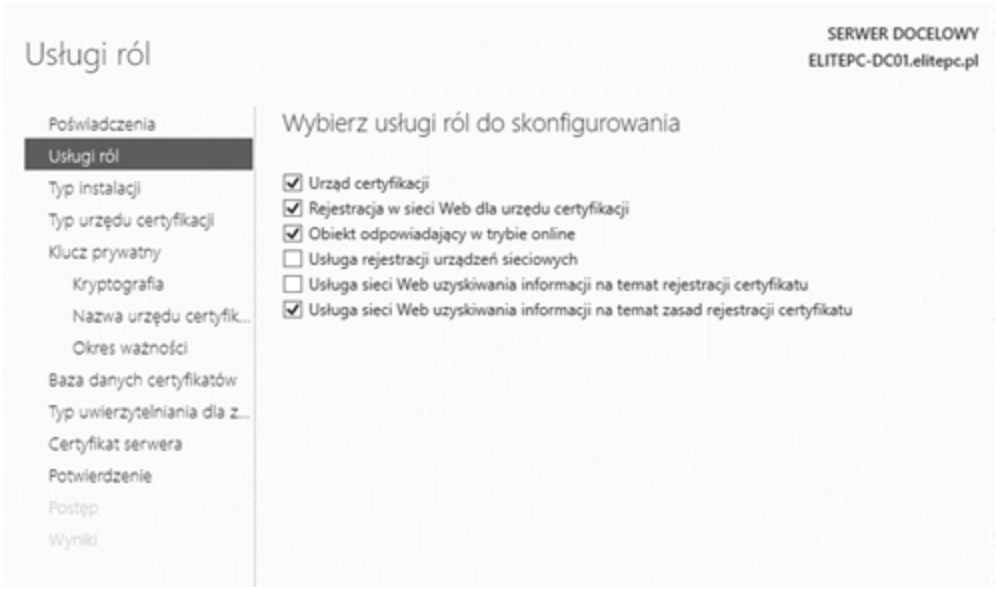
Niezbędna będzie dodatkowa konfiguracja, do której wchodzi się poprzez Centrum Akcji (Action Center).



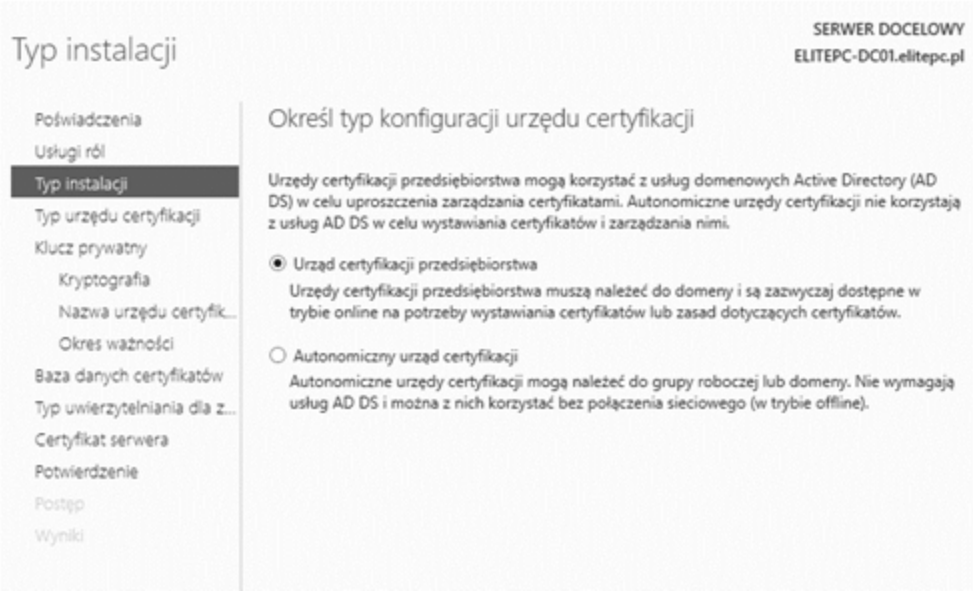
W pierwszej karcie nowo otwartego kreatora należy podać dane użytkownika, który będzie miał stosowne uprawnienia do przeprowadzenia konfiguracji.



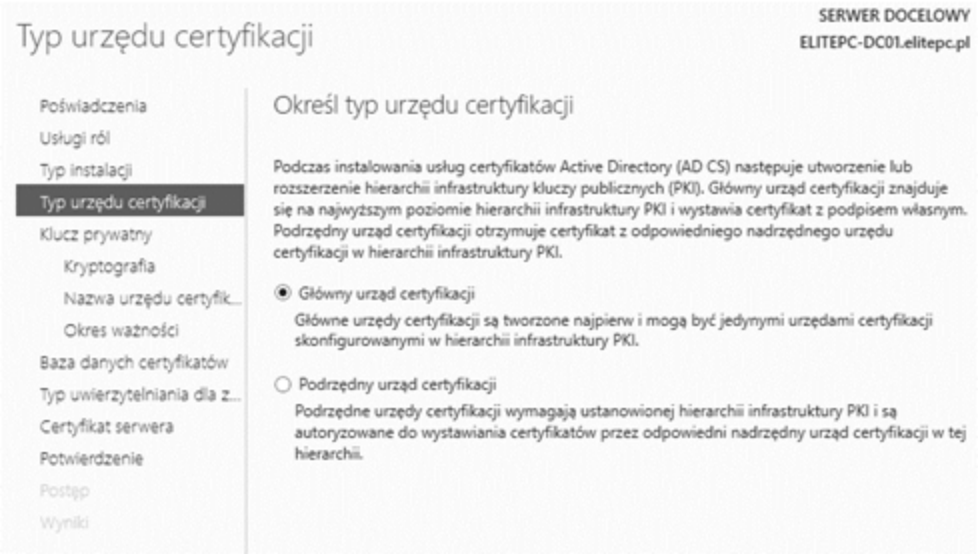
Na kolejnej karcie wystarczy, że zostanie skonfigurowany Urząd Certyfikacji (Certification Authority), jednak wraz z nim można skonfigurować pozostałe usługi wybrane na zrzucie ekranowym. Dwie inne wybrane opcje wymagają odrębnej konfiguracji po uruchomieniu CA.



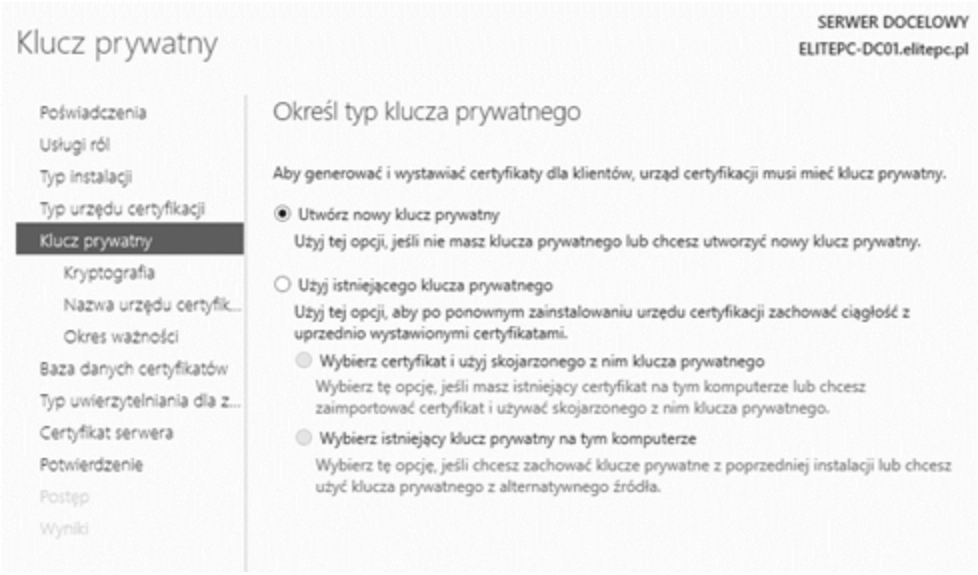
Następnie należy zdefiniować rodzaj CA. Enterprise wymaga do działania AD, natomiast w Standalone CA może nie być powiązany z AD i służyć np. jedynie jako uzupełnienie serwera hostingowego. Jako że serwer ćwiczeniowy korzysta z AD, zostanie wybrana opcja Enterprise.



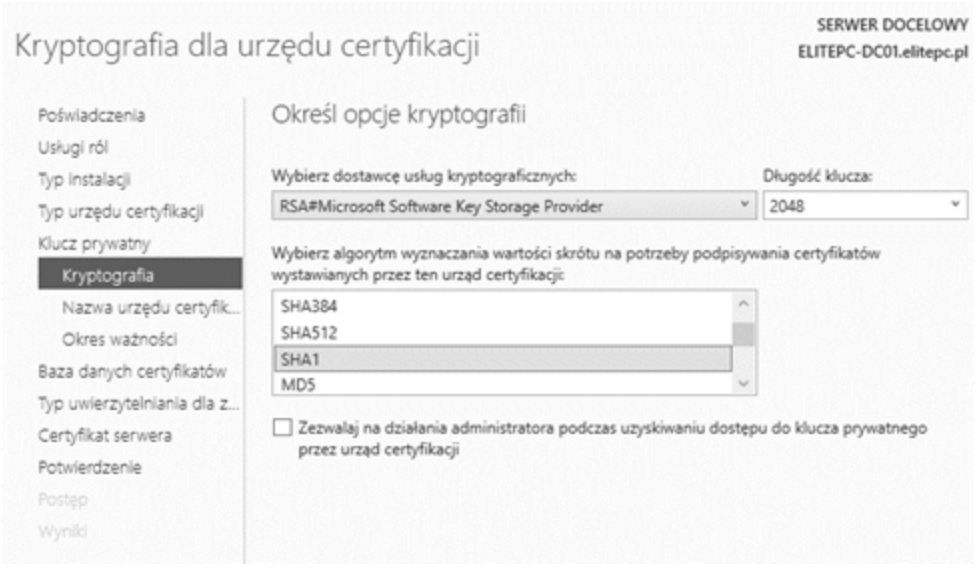
W następnym kroku należy zdefiniować, czy jest to Główny serwer CA (Root CA) czy Podrzędny / Zapasowy (Subordinate CA). W tym przypadku jest to jednak serwer główny.



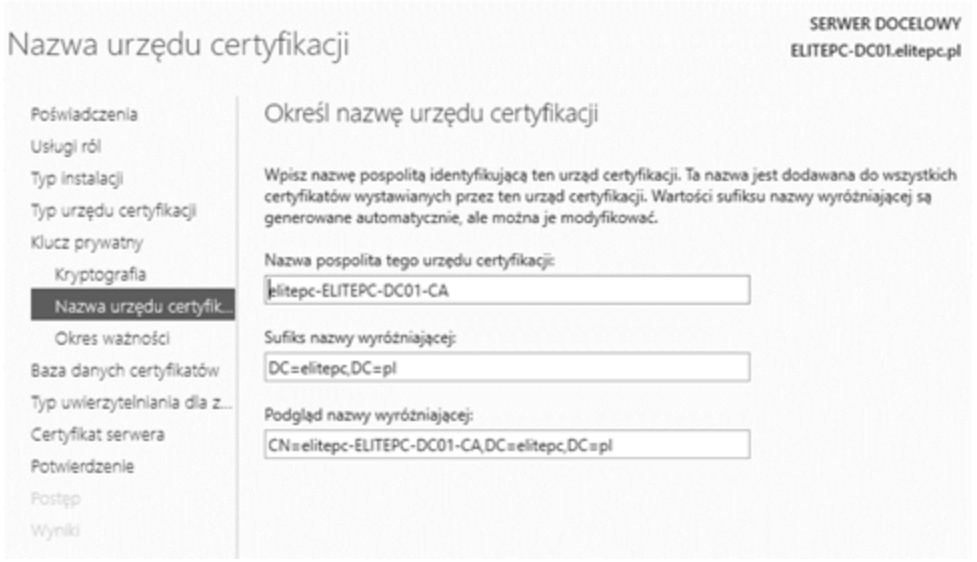
W kolejnym kroku zostanie stworzony Klucz Prywatny (Private Key). Gdyby taki już istniał, byłaby możliwość użycia go (Use existing private key). Jako że ma zostać stworzony, należy wybrać opcję pierwszą Stwórz nowy klucz prywatny (Create a new private key).



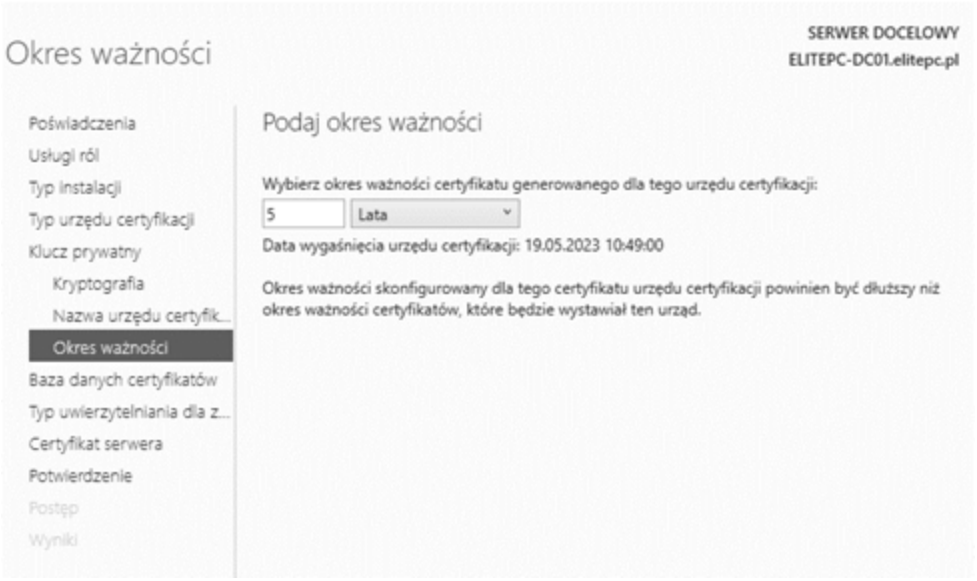
Na kolejnej karcie istnieje możliwość wybrania metody kryptografii. Jeżeli administrator nie zgłębił tego tematu i nie ma zbyt dużej wiedzy o metodach kryptografii, najlepiej będzie zostawić ustawienia domyślne.



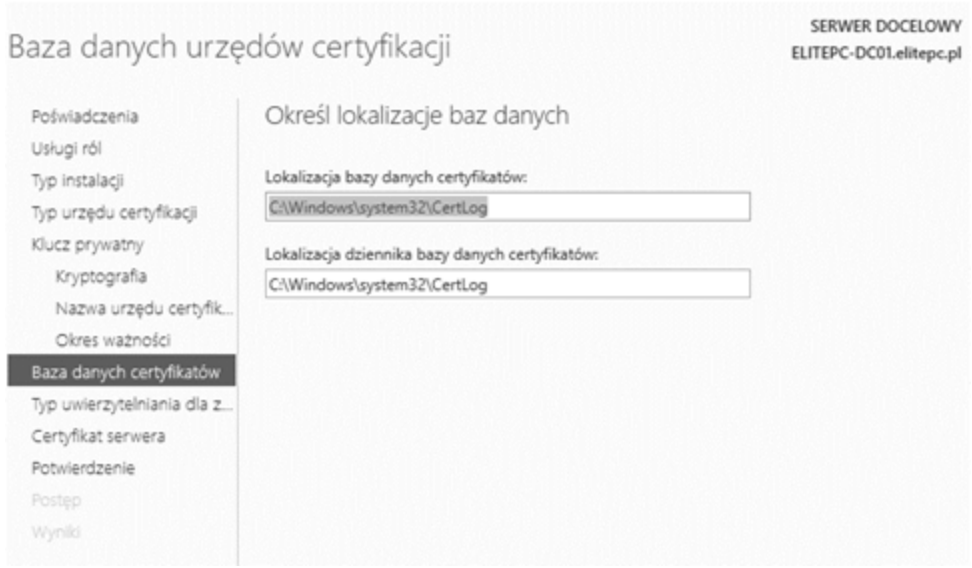
W kolejnym oknie należy zdefiniować informacje i nazwy związane z CA. Informacje te znajdą się w certyfikatach.



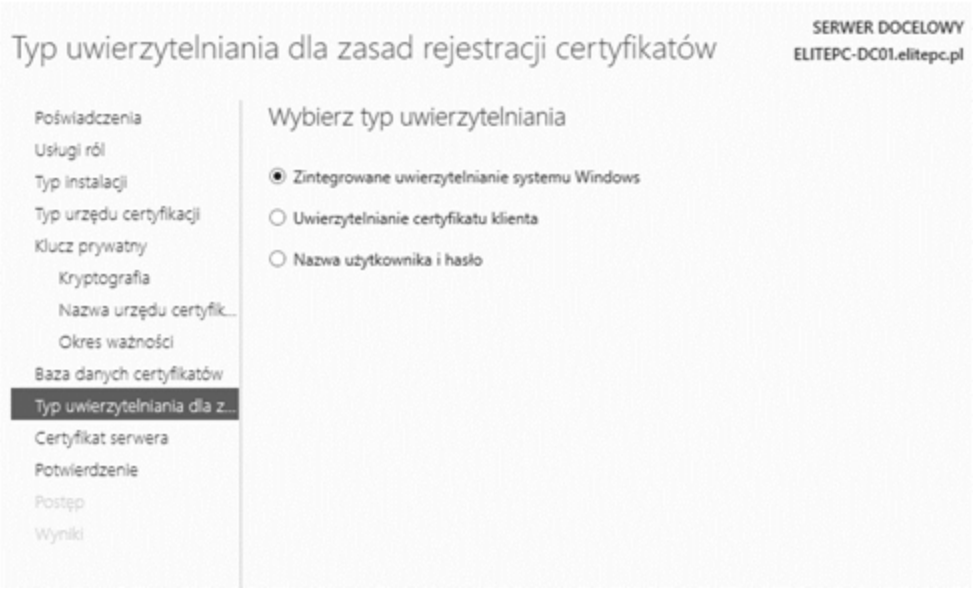
Następnie trzeba zdefiniować okres ważności certyfikatu. Domyślnie jest to 5 lat.



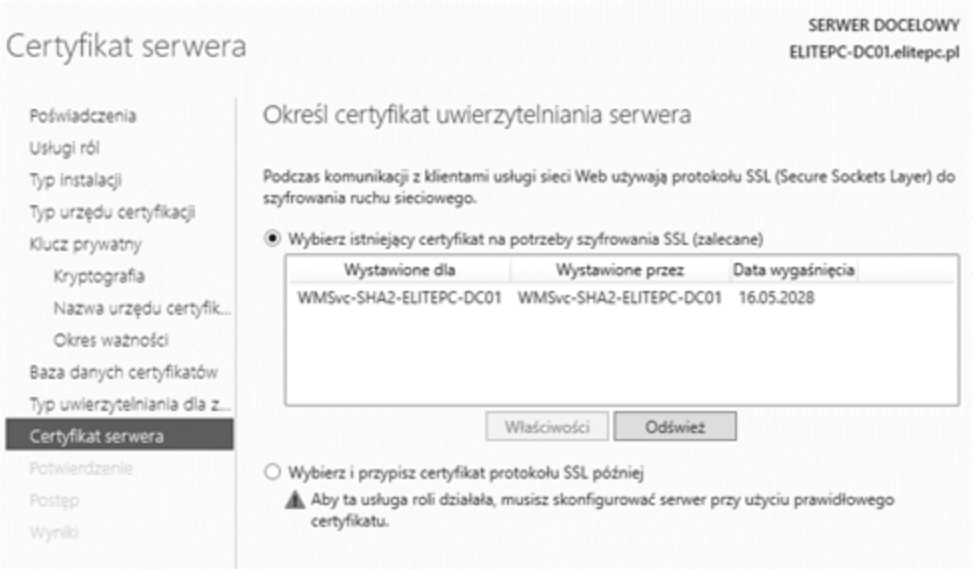
W kolejnym kroku należy wybrać miejsce przechowywania logów i bazy danych.



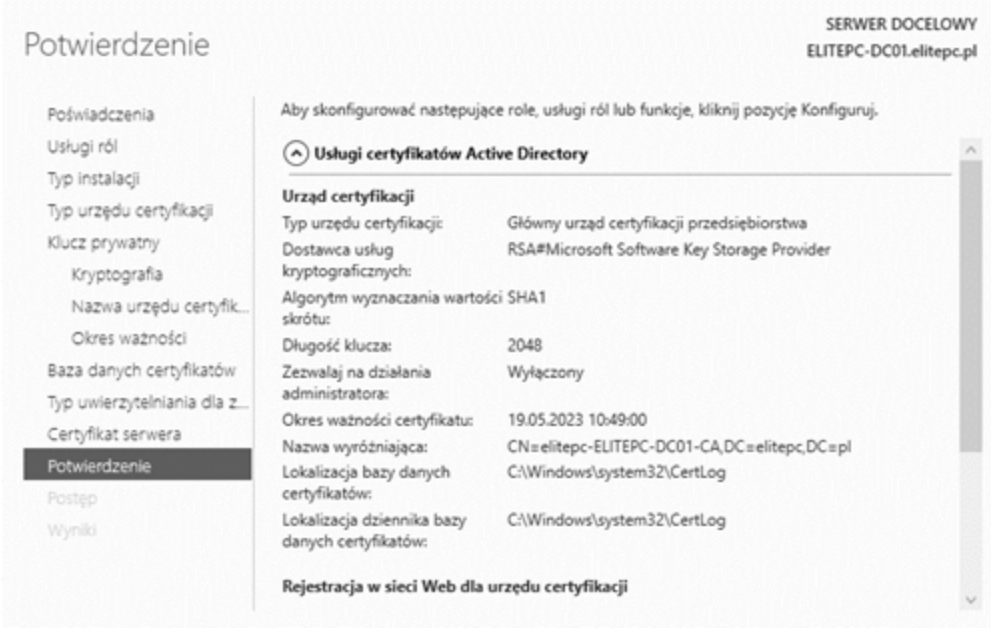
W następnym oknie konieczne jest zdefiniowanie metody autentykacji użytkowników. Dla komputerów pracujących w domenie najlepszym wyborem będzie Zintegrowane uwierzytelnianie systemu Windows (Windows integrated authentication).



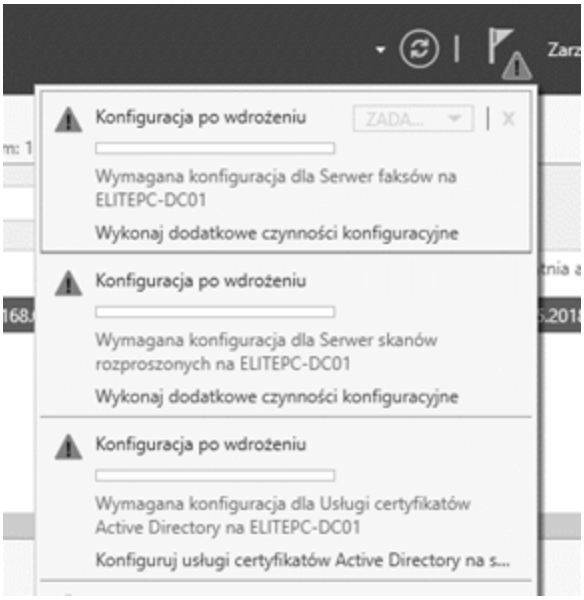
W kolejnym oknie należy wybrać certyfikat, który będzie używany do szyfrowania połączenia pomiędzy klientami a serwerem.



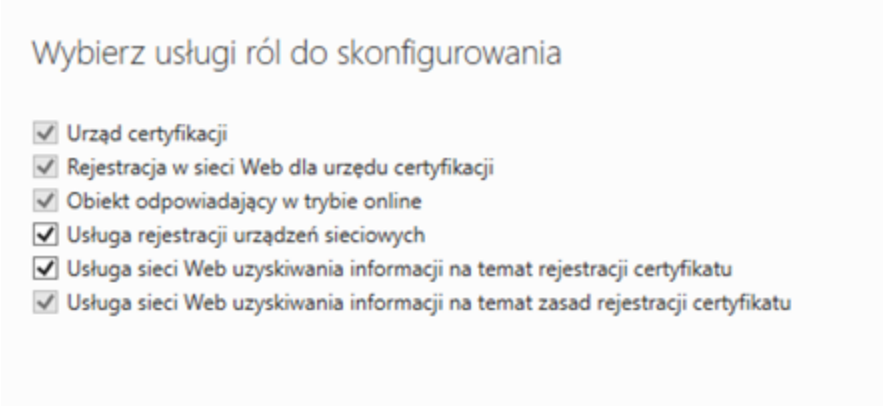
Na karcie podsumowującej należy wybrać Konfiguruj (Configure). Po tym kroku warto uruchomić ponownie serwer.



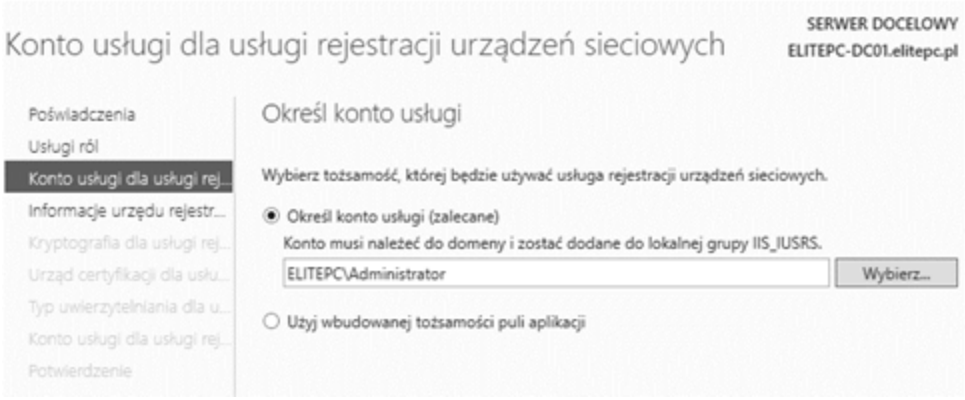
Teraz, poprzez centrum akcji, należy ponownie uruchomić kreatora konfiguracji CA.



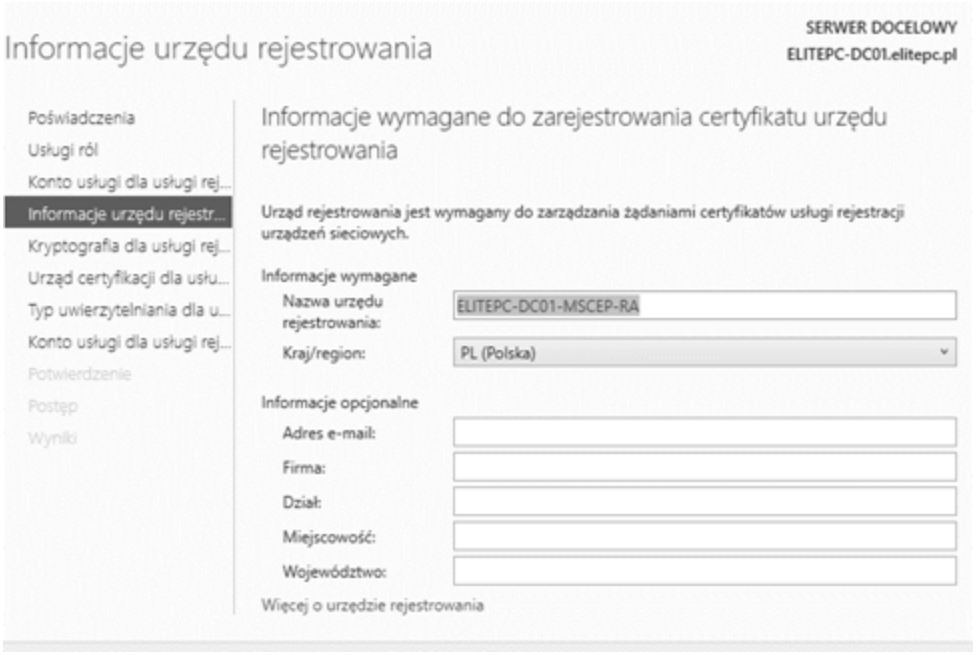
Tym razem z listy usług konieczne jest wybranie dwóch opcji, których wcześniej nie można było zainstalować.



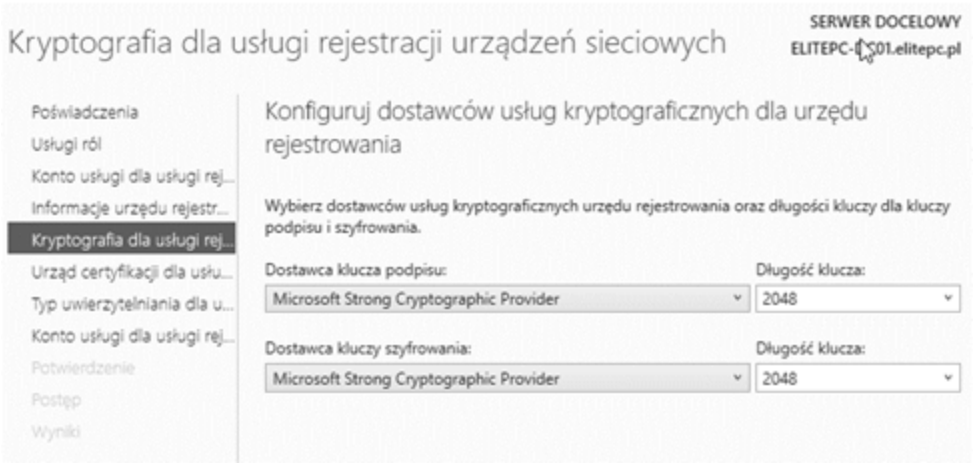
Następnie należy wybrać konto użytkownika, który ma uprawnienia do przeprowadzenia wymaganych zadań. Musi on należeć do grupy IIS_IUSRS. Można więc dodać do tej grupy administratora i wykorzystać jego konto.



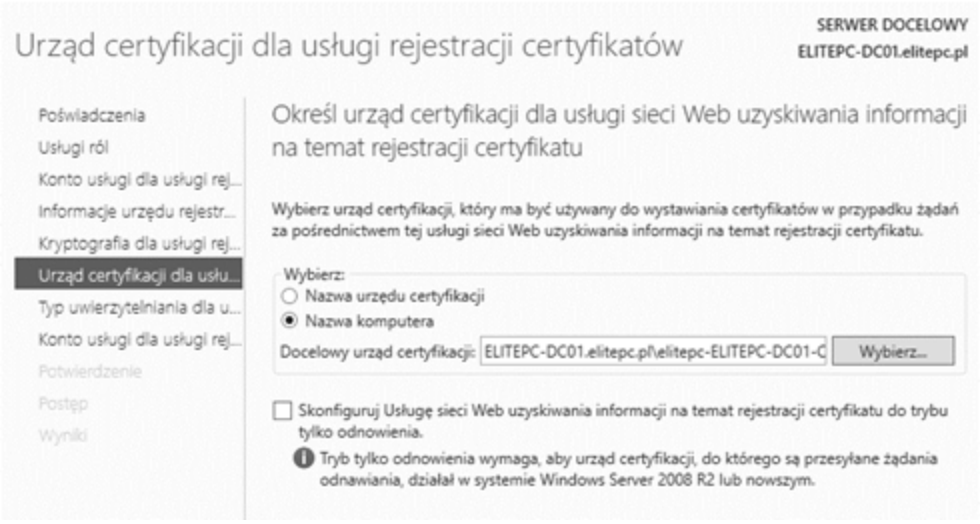
W kolejnym oknie konieczne jest wprowadzenie informacji dotyczących przedsiębiorstwa.



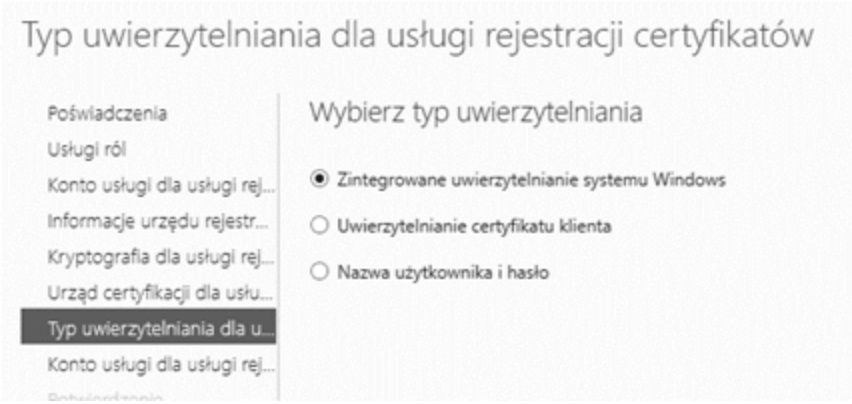
Następnie należy wybrać dostawcę (provider) kryptografii wraz z długością klucza szyfrującego.



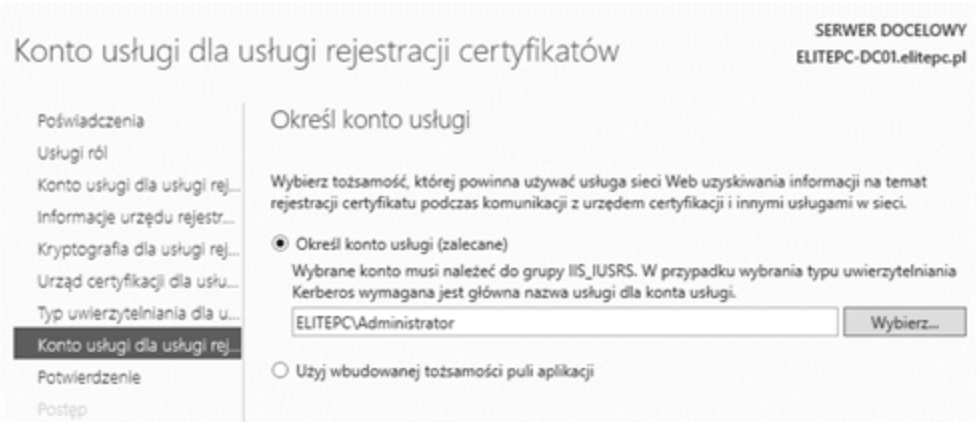
Teraz należy przejść do części kreatora odpowiedzialnej za konfigurację zapisów certyfikatów w sieci Web. Konieczne jest wybranie opcji Nazwa komputera (Computer name) i wskazanie wcześniej skonfigurowanego CA.



Kolejnym krokiem jest wybór metody autentykacji. Tak jak wcześniej, należy pozostawić tę opcję domyślną, tj. Zintegrowane uwierzytelnianie systemu Windows (Windows integrated authentication).

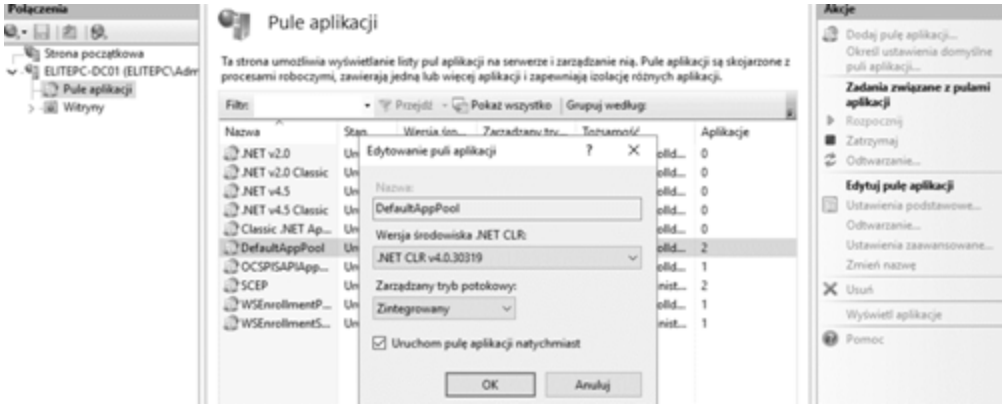


Należy teraz zdefiniować konto użytkownika, który będzie odpowiadał za komunikację między CES a CA. Na potrzeby książki będzie to Administrator. Następnie na karcie podsumowującej należy kliknąć w Konfiguruj (Configure), a po chwili w Zamknij (Close).



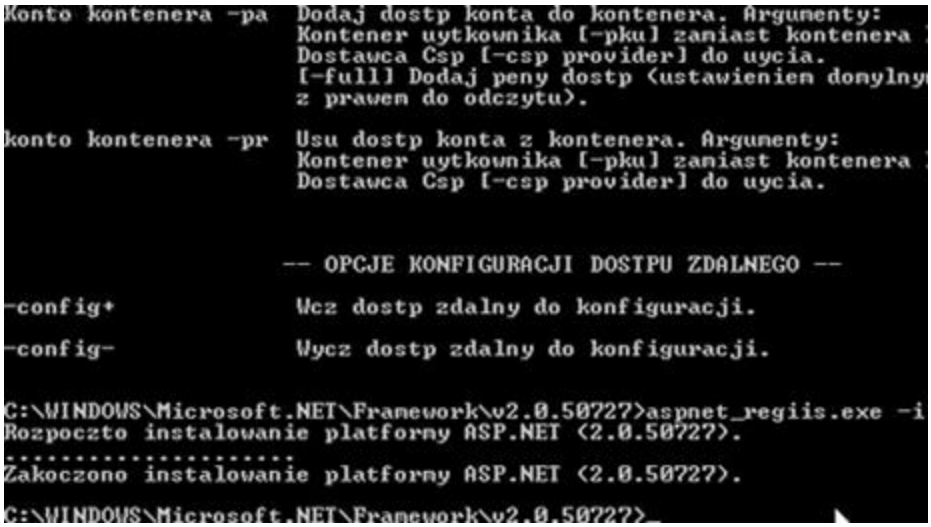
6.3. Aktualizacja platformy .NET

Gdy urząd certyfikacji będzie już zainstalowany i skonfigurowany, warto wrócić do menadżera IIS. W sekcji Pule aplikacji (Application Pool) .NET można ustawić platformę .NET Framework, jaką ma domyślnie używać serwer – będzie to wersja 4.0. Aby nowsza wersja była dostępna w tym oknie, konieczne jest pobranie jej z Internetu i zainstalowanie.



Jeśli dana wersja nie będzie widoczna, konieczne stanie się wykonanie w konsoli odpowiedniego polecenia

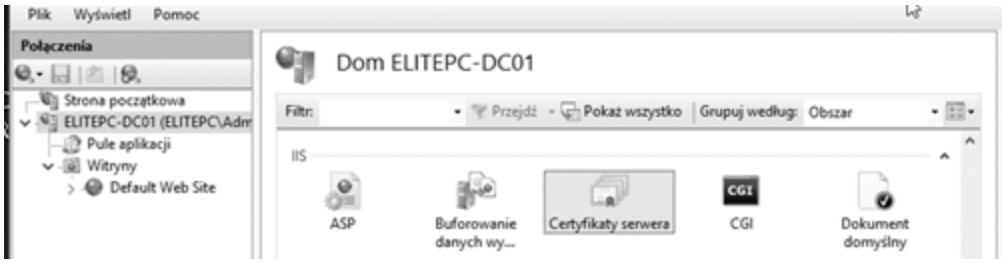
odpowiadającego za instalację ASP.NET.



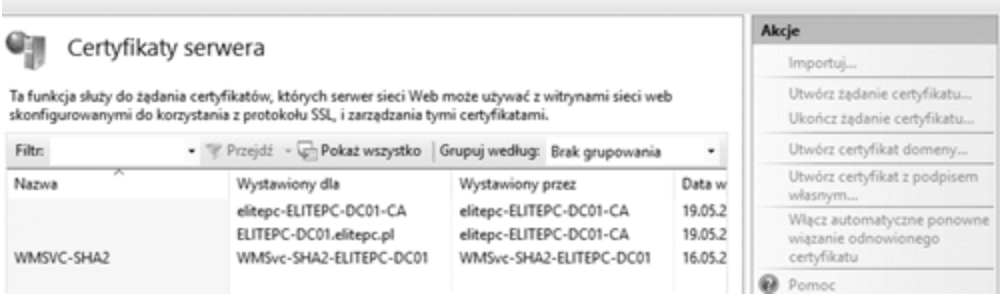
6.4. Tworzenie nowych certyfikatów

Podstawowe opcje logowania można ustawić, klikając w ikonę Uwierzytelnianie (Authentication) po wcześniejszym wybraniu w prawym menu pożądanej witryny sieci Web.

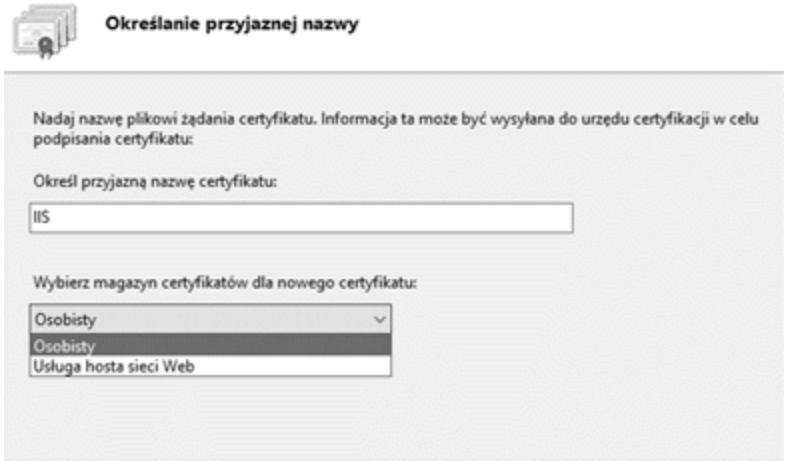
Warto jednak wcześniej wrócić o poziom wyżej i klikając na nazwę serwera w drzewie po lewej stronie, przejść do ogólnych ustawień serwera. Poza konfiguracją IIS znajduje się tam wiele innych opcji, np. te związane z bezpieczeństwem, FTP oraz inne. W tym dziale strona zostanie zabezpieczona certyfikatem, a następnie logowaniem. Pierwszym krokiem będzie stworzenie jakiegoś certyfikatu dla serwera. Należy kliknąć Certyfikaty Serwera (Server Certificates).



Następnie należy kliknąć Utwórz Certyfikat z Podpisem Własnym (Create Self-Signed Certificate). Dzięki temu uniknie się potrzeby odwoływania do głównego urzędu certyfikacji w domenie.

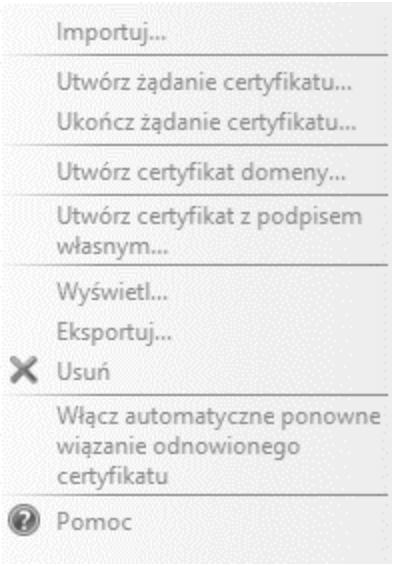


Pojawi się kreator, w którym należy podać nazwę oraz wybrać przeznaczenie certyfikatu, czyli: Użytek własny (Personal) lub Hosting WWW (Web Hosting).

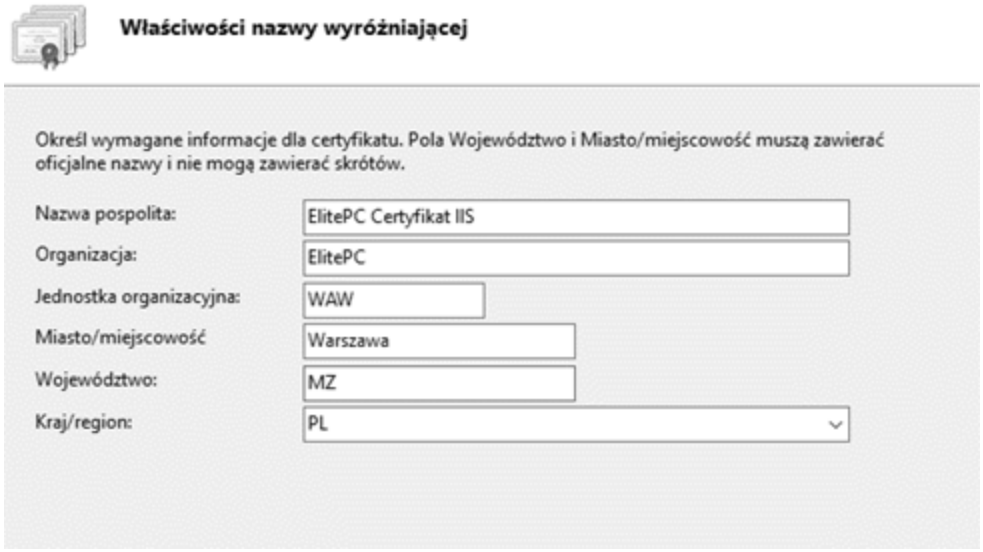


Następnie należy kliknąć w OK.

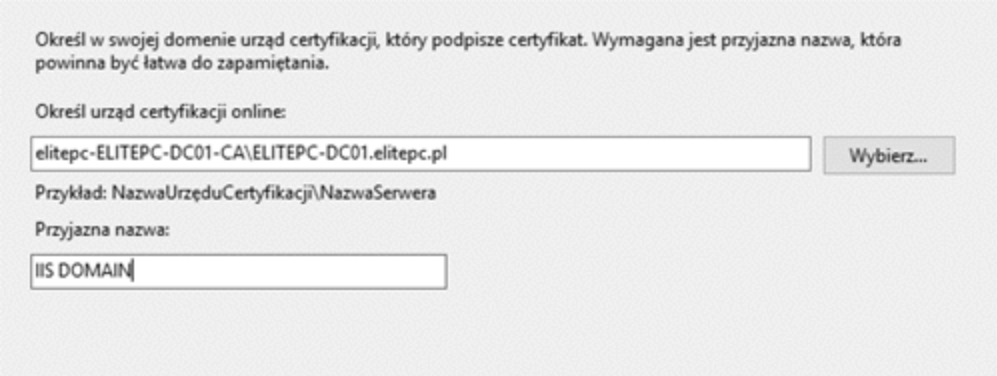
Mając już zainstalowany CA, łatwo jest także utworzyć Certyfikat domeny (Domain Certificate). Krok ten mogą pominąć osoby, którym wystarcza certyfikat z podpisem własnym, jaki wcześniej został utworzony. Certyfikat domeny tworzy się, wybierając opcję Stwórz certyfikat domeny (Create Domain Certificate).



Na pierwszej karcie kreatora należy wypełnić dane dotyczące organizacji.

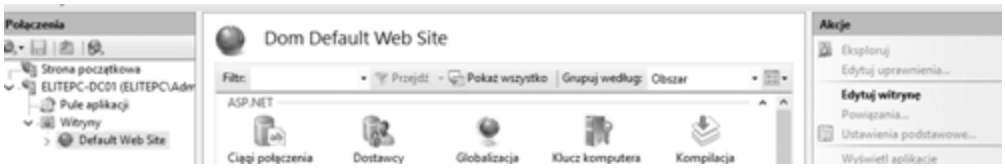


Następnie definiuje się urząd certyfikacji, który ma zostać wykorzystany, oraz należy podać przyjazną nazwę dla certyfikatu. W kolejnym kroku trzeba kliknąć Zakończ (Finish).



6.5. Zarządzanie Serwerem IIS

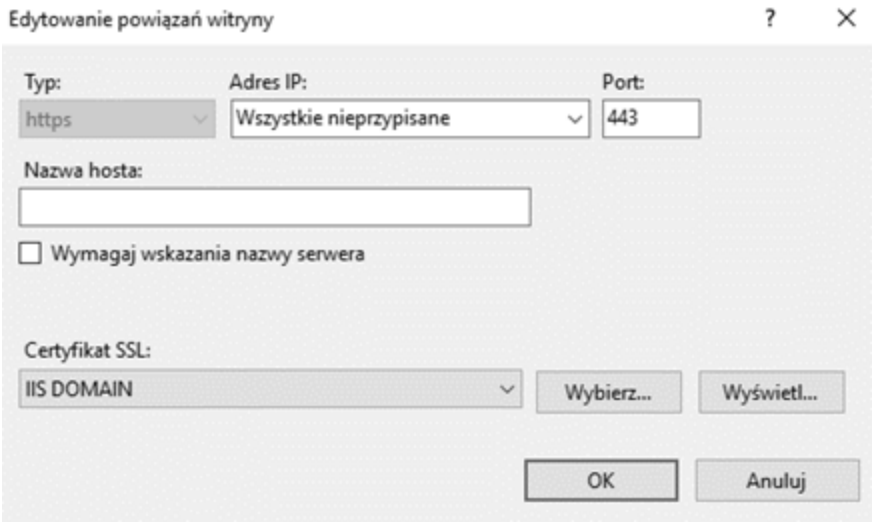
W przypadku książkowym pozostało już jedynie podłączyć certyfikat do danej witryny. Należy kliknąć najpierw na liście nazwę witryny, a następnie wybrać z menu po prawej opcję: Powiązania (Bindings).



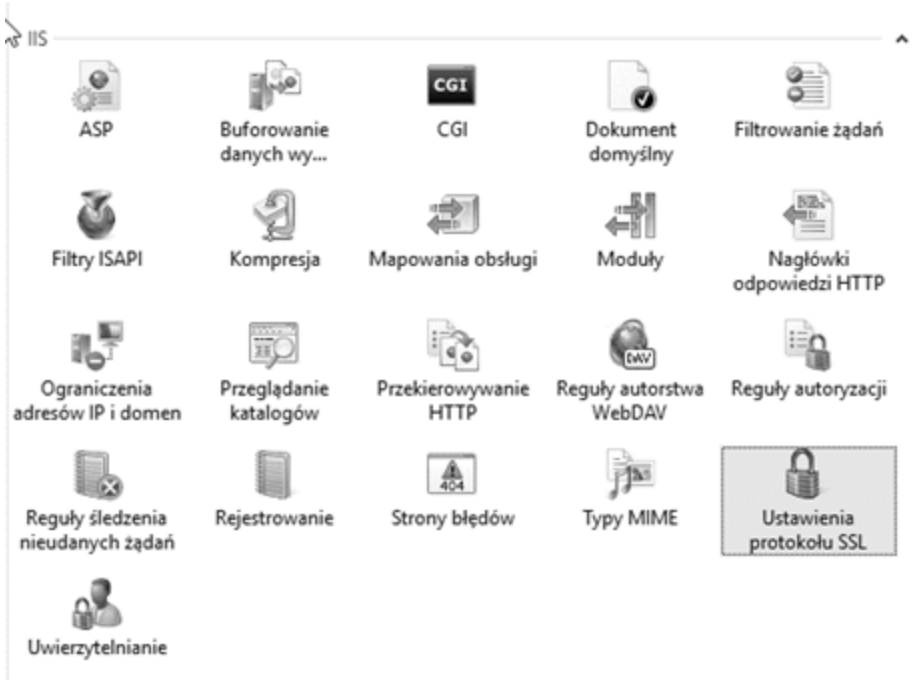
Na ekranie, który się pojawi, należy kliknąć Dodaj (Add).

Jego typ należy ustawić na https i wybrać utworzony wcześniej certyfikat serwera. Wybranie w polu Adres IP opcji Wszystkie nieprzypisane (All unassigned) powoduje tyle, iż na każdej karcie sieciowej na porcie 443, będzie używany ten, a nie inny certyfikat. Skasowanie powiązania

HTTP spowoduje, że nie będzie można podłączyć się do serwera w niezabezpieczony sposób. Warto też wtedy zablokować port w zaporze. Można także na zwykłej stronie stworzyć planszę informującą, że serwer wymaga certyfikatu wraz z przekierowaniem. Opcje te można zawsze zmienić przyciskiem edycji.

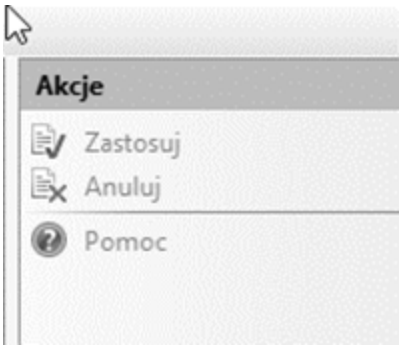


Inną metodą będzie wymuszenie wymagania certyfikatu SSL. Aby tego dokonać, należy kliknąć w opcję Ustawienia Protokołu SSL (SSL Settings).



Na planszy, która się pojawi, należy wybrać opcję Wymagaj Certyfikatu SSL (Require SSL) oraz zdefiniować dogodne ustawienia klienta. Zaleca się wybranie opcji Akceptuj (Accept).

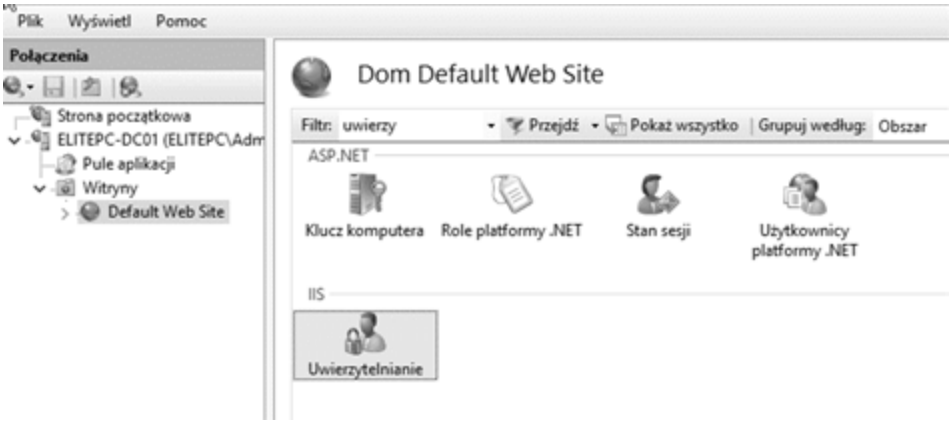
Po wprowadzeniu ustawień, należy kliknąć Zastosuj (Apply) w menu po prawej stronie.



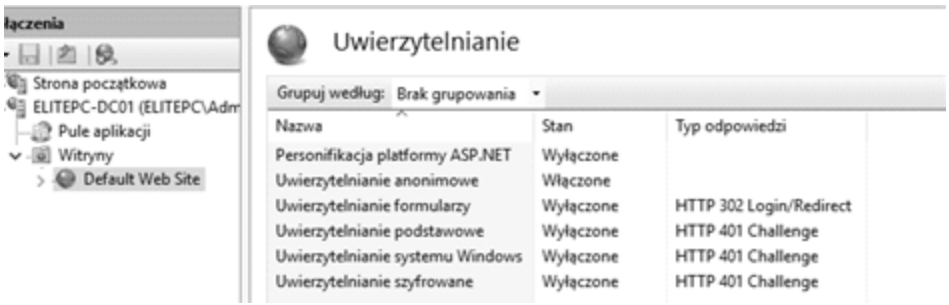
Teraz każda próba wejścia na witrynę innym portem niż SSL zakończy się błędem i jednocześnie automatycznie wyświetli informacje na temat dalszego postępowania dla użytkownika.

Po wpisaniu w belce adresu przedrostka https:// strona www powinna się załadować, a komunikacja powinna odbyć się w sposób szyfrowany. Naturalnie, będzie konieczna akceptacja certyfikatu.

Warto także zabezpieczyć stronę przed niepowołanymi odwiedzinami. W tym celu należy kliknąć dwukrotnie w ikonę Uwierzytelnianie (Authentication).



Wyłączone też zostanie Uwierzytelnianie anonimowe (Anonymous Authentication). Aby je wyłączyć, należy kliknąć przycisk Wyłącz (Disable) z prawej strony.



Uwierzytelnianie w sieci odbywa się na zasadzie komunikacji między serwerem a przeglądarką, podczas której przesyłane są nagłówki protokołu http oraz komunikaty o błędach.

Komunikacja przebiega następująco:

1. Przeglądarka zgłasza żądanie, np. HTTP-GET.

2. Serwer sprawdza, czy obowiązkowe jest uwierzytelnienie. Jeśli sprawdzenie się nie powiedzie, ponieważ uwierzytelnienie jest niezbędne, serwer odpowiada komunikatem o błędzie podobnym do tego poniżej:

Brak upoważnienia do wyświetlania tej strony

Nie masz uprawnień, by przeglądać ten katalog lub tę stronę przy użyciu podanych poświadczeń. Komunikat ten zawiera informacje, których przeglądarka sieci Web może użyć do ponownego przesłania żądania, jako żądania uwierzytelnionego.

3. Przeglądarka, na podstawie tego, co odpowie serwer, tworzy nowe żądania, które zawierają informacje o uwierzytelnianiu.

4. Serwer sieci Web dokonuje sprawdzenia uwierzytelnienia. Jeśli sprawdzenie powiedzie się, serwer sieci Web odsyła do przeglądarki dane, których pierwotnie żądano.

Istnieją następujące metody uwierzytelniania:

– Uwierzytelnianie anonimowe (Anonymous Authentication) – w celu uwierzytelnienia użytkowników anonimowych, którzy żądają zawartości sieci, usługi IIS tworzą konto IUSR_nazwa_komputera. Konto to użytkownikowi daje uprawnienia do zalogowania się lokalnie. Istnieje możliwość zresetowania dostępu anonimowych użytkowników w taki sposób, aby używali dowolnego konta z systemu Windows.

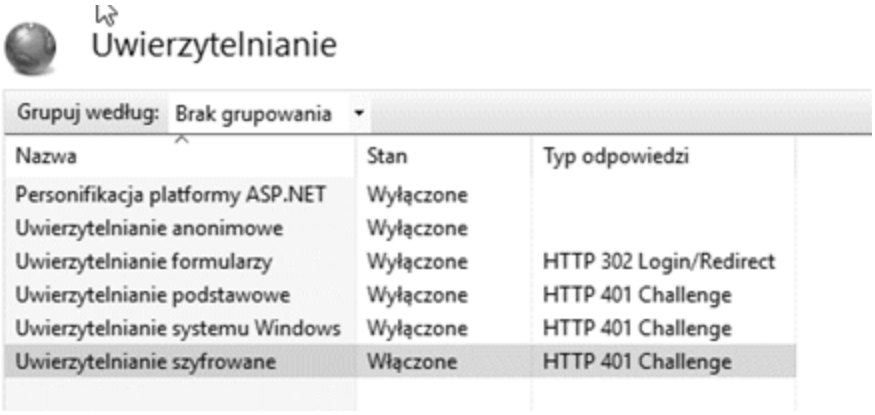
– Uwierzytelnienie podstawowe (Basic Authentication) – wykorzystywane jest do ograniczania dostępu do danych na serwerze znajdujących się na dysku sformatowanym w systemie NTFS. Jeśli używa się podstawowego uwierzytelniania, użytkownik ma obowiązek wprowadzenia poświadczeń, a możliwość dostępu jest zależna od identyfikatora użytkownika. Aby móc korzystać z podstawowego uwierzytelniania, każdy użytkownik musi mieć nadane prawo do logowania się lokalnie.

– Zintegrowane uwierzytelnianie systemu Windows (Windows Authentication) – uwierzytelnianie to zapewnia wyższy poziom bezpieczeństwa niż uwierzytelnianie podstawowe. Bardzo dobrze sprawdza się w środowisku intranetowym, w którym użytkownicy mają domenowe konta systemu Windows. W przypadku zintegrowanego

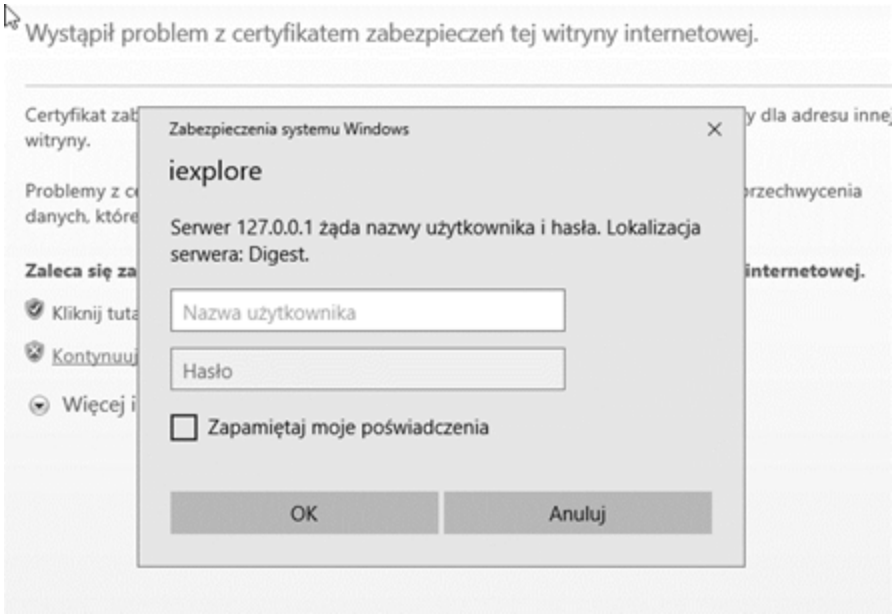
uwierzytelniania systemu Windows, przeglądarka w miarę możliwości używa bieżących poświadczeń użytkownika, które wcześniej były już używane do logowania się do domeny. Jeżeli użycie tych poświadczeń nie powiedzie się, wyświetlona zostanie odpowiednia informacja i użytkownik zostanie poproszony o podanie poprawnych danych logowania. Przy zintegrowanym uwierzytelnianiu systemu Windows hasło użytkownika nie jest przesyłane do serwera. Jeżeli użytkownik został zalogowany do komputera jako użytkownik domeny, to gdy będzie próbował się dostać do sieciowego komputera w tej domenie, nie ma konieczności ponownego uwierzytelniania.

– Uwierzytelnianie szyfrowane (Digest Authentication) – eliminuje liczne wady uwierzytelnienia podstawowego. Podczaj jego używania, uwierzytelnianie jest szyfrowane. W szyfrowanym uwierzytelnianiu używany jest mechanizm wezwania/odpowiedzi (identyczny mechanizm używany jest w zintegrowanym uwierzytelnianiu systemu Windows), a hasła są przesyłane w formacie zaszyfrowanym. Aby użyć uwierzytelniania szyfrowanego, koniecznością wszystkich kont użytkowników jest posiadanie odpowiedniej konfiguracji z włączoną opcją Zapisz hasła dla wszystkich użytkowników w domenie, korzystając z szyfrowania odwracalnego. W momencie gdy została włączona ta opcja, należy zresetować lub wprowadzić ponownie hasło.

Zostanie wybrana jakaś metoda uwierzytelniania. Najlepsze będzie szyfrowanie. Zostanie więc ono włączone po kliknięciu Włącz Włącz (Enabled) po prawej stronie.

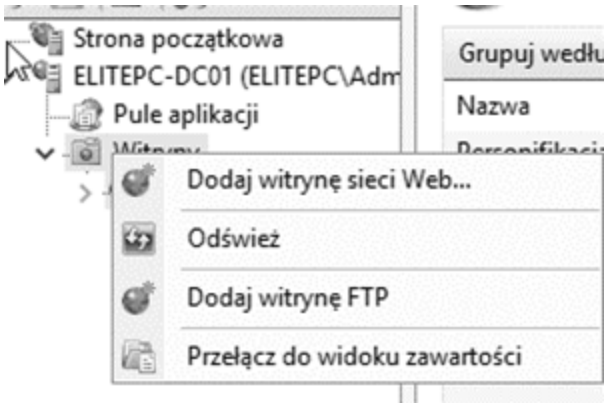


Pojawi się ekran logowania po odświeżeniu strony. Należy wprowadzić swój login i hasło.

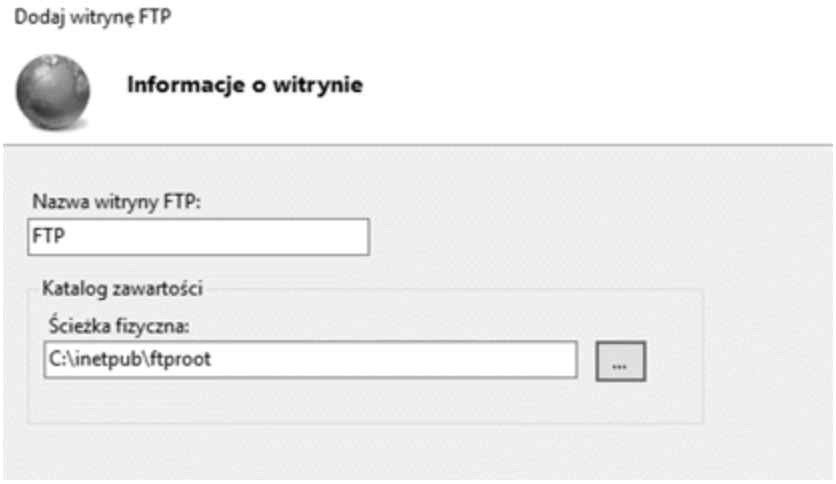


6.6. Uruchamianie Serwera FTP

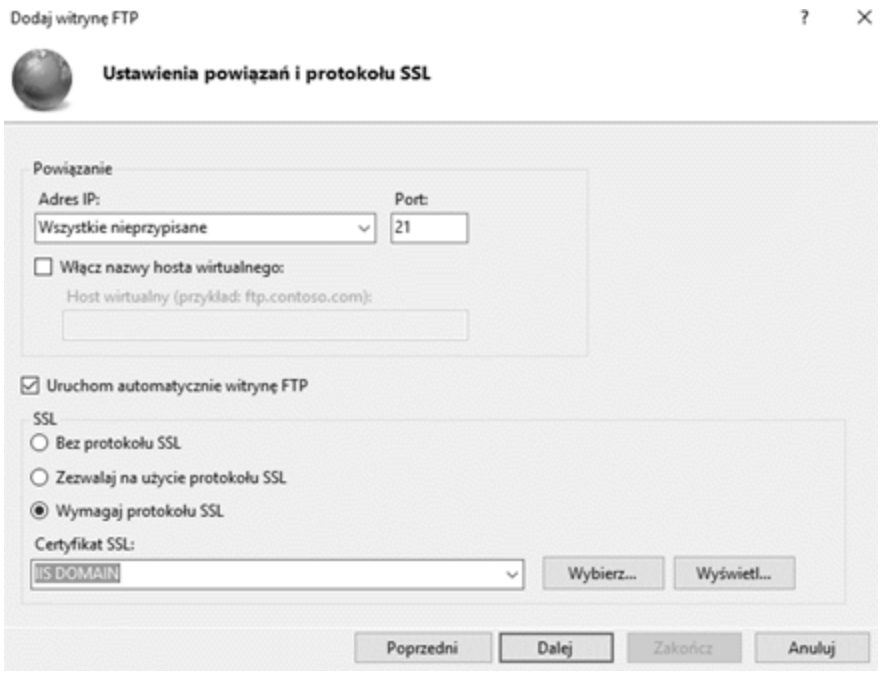
Uruchomiony zostanie teraz serwer FTP, który także, w dalszej części książki, zostanie zabezpieczony. W tym celu należy kliknąć prawym przyciskiem myszy na napisie Witryny (Site) i dodać Nową Witrynę FTP (Add FTP Site).



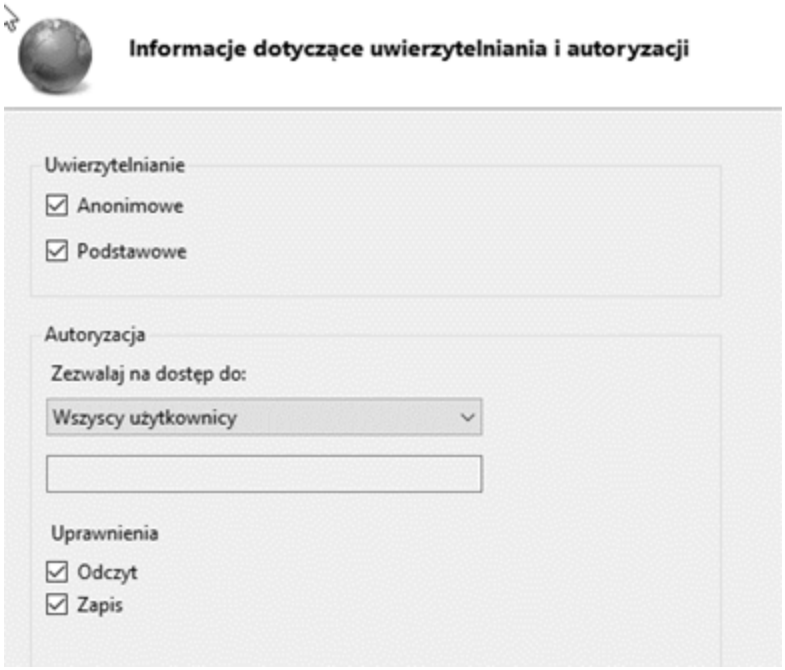
Na kolejnej karcie należy podać nazwę witryny oraz ścieżkę na dysku, gdzie będzie ona przechowywała swoje dane.



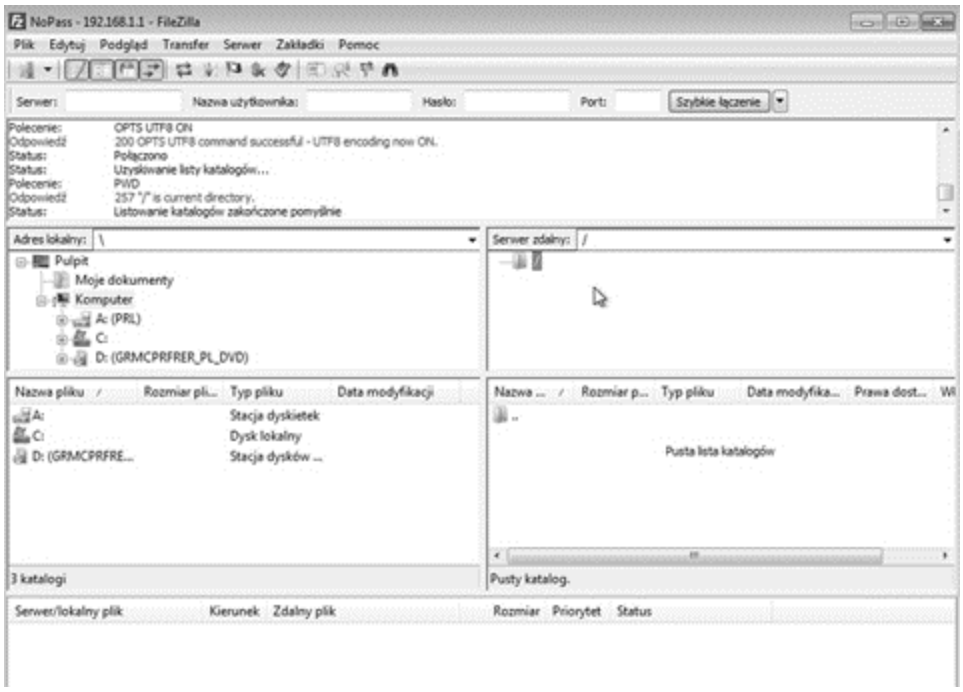
Na następnej karcie pozostawione będą opcje domyślne.



Pozwolono też na Uwierzytelnianie anonimowe (Anonymous).

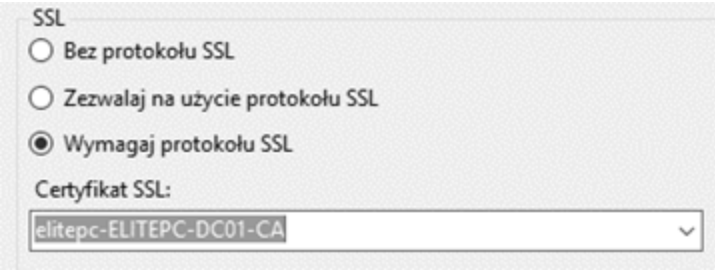


Do testów połączeń wykorzystany zostanie program FileZilla, zainstalowany na komputerze klienckim.

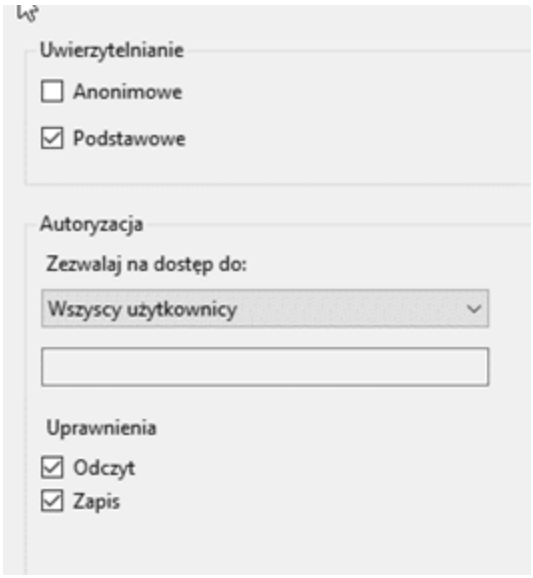


Warto także skupić się na zabezpieczeniu serwera FTP. Ponownie zostanie stworzony certyfikat z własnym podpisem, tym razem dla serwera FTP.

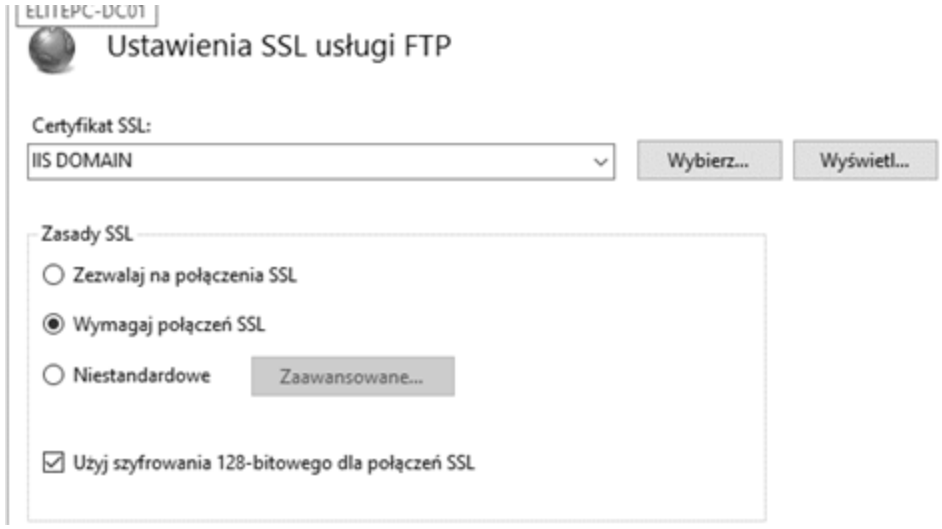
Zostanie skasowana strona FTP, będzie trzeba przejść kreator raz jeszcze. Tym razem zostanie włączony certyfikat SSL i wybrany podany wcześniej certyfikat.



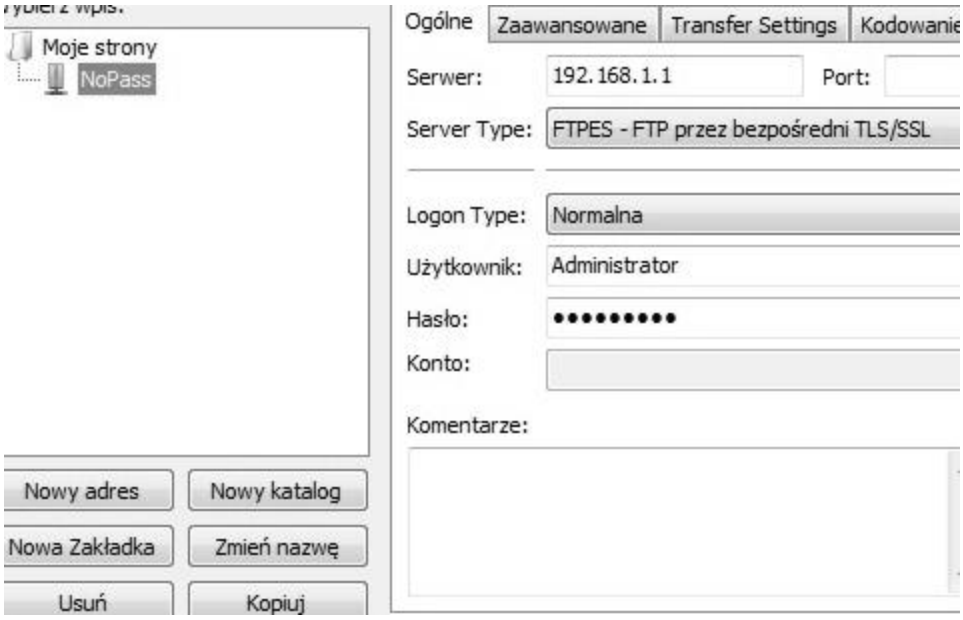
Uwierzytelnianie anonimowe nie jest pożądane, zostanie więc wyłączone.



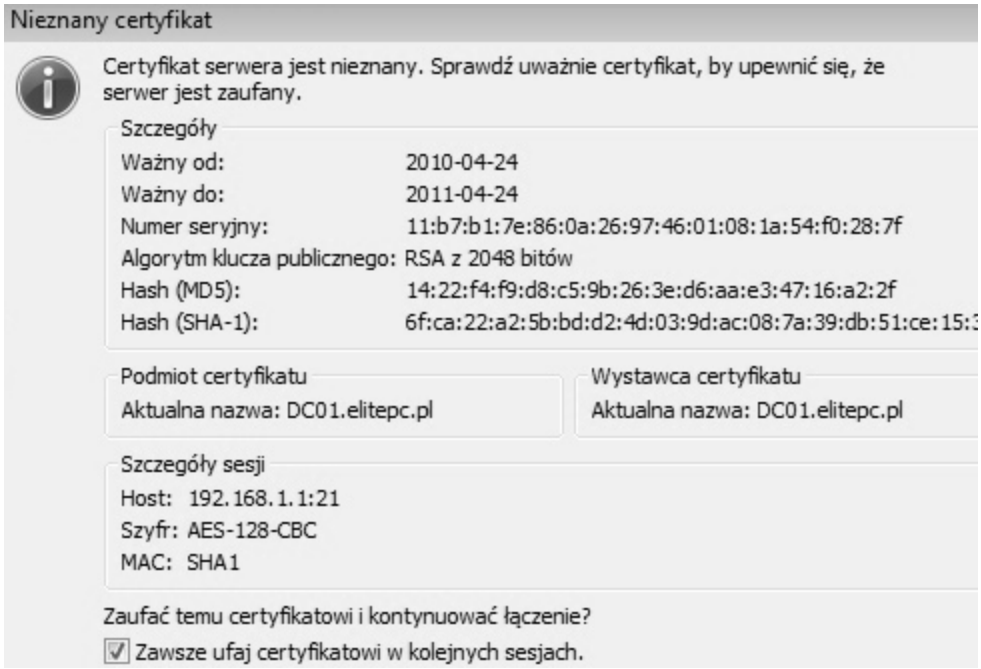
Należy wejść w Ustawienia SSL usługi FTP (FTP SSL Settings), wybrać Wymagaj połączeń SSL (Require SSL Connections) i zaznaczyć Szyfrowanie 128 bitowe (Use 128-bit encryption for SSL connections).



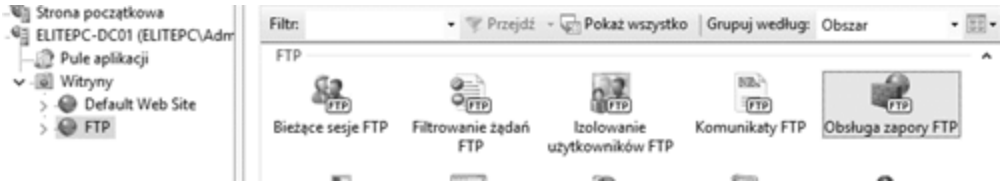
Klienta FTP konfiguruje się w następujący sposób:



Należy zaakceptować certyfikat i po chwili następuje bezpieczne połączenie z FTP.



To jednak nie wszystko. Aby FTP działał poza siecią lokalną, należy jeszcze skonfigurować Firewall. Trzeba znaleźć Obsługę zapory FTP (FTP Firewall Support).



Należy ją skonfigurować tak, że adres IP to publiczny adres IP. Zakres portów, jaki należy ustawić to: 49152-65535. Gdyby pojawiły się problemy z routingiem, czasami pomogą konsolowe komendy:

Dla FTP niezabezpieczonego:

netsh advfirewall firewall add rule name="FTP (non-SSL)" action=allow protocol=TCP dir=in localport=21

netsh advfirewall set global StatefulFtp enable

Dla zabezpieczonego SSL'em:

netsh advfirewall firewall add rule name="FTP for IIS7" service=ftpsvc action=allow protocol=TCP dir=in

netsh advfirewall set global StatefulFtp disable

6.7. IIS i PHP

We wcześniejszych działach został zainstalowany IIS oraz serwer FTP. Ten serwer jednak nie wspierał stron napisanych w języku PHP. Można to jednak łatwo zmienić.

PHP może funkcjonować przy użyciu protokołu ISAPI lub CGI. Wadą CGI jest to, że dla każdego żądania tworzony jest w systemie osobny proces, co przy wielu użytkownikach podłączonych jednocześnie,- w znacznym stopniu obciąża

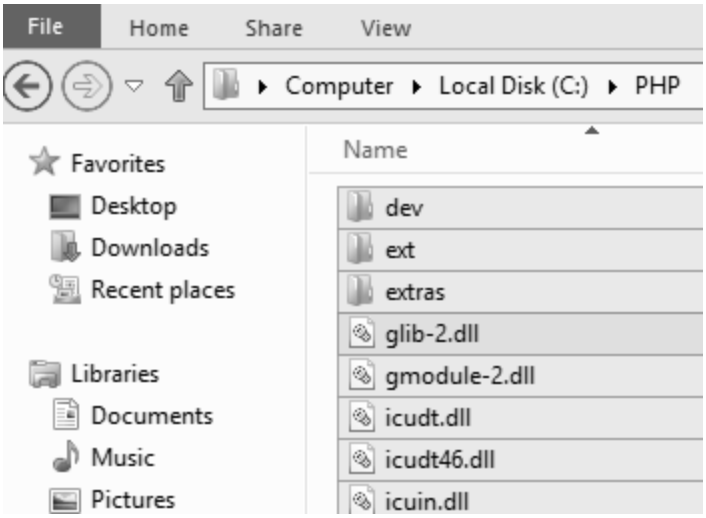
komputer. ISAPI jest wolne od tej wady, ponieważ wykorzystuje wewnętrzne procesy serwera IIS. Jego wadą jest to, że nie radzi on sobie z wielowątkowością, do której obsłużenia używa się bibliotek PHP, co znów prowadzi do utraty wydajności. Dlatego też w Windows Server 2008 Microsoft zaimplementował trzecie i najlepsze rozwiązanie – FastCGI. Zostało ono również przeniesione do Windows Server 2016.

Pierwszym krokiem instalacji będzie dodanie roli serwera IIS. Jako że wcześniej zostały już zainstalowane wszystkie możliwe komponenty, ten krok można pominąć. Jeżeli jednak zaczyna się od początku, należy zaznaczyć Serwer sieci Web i kliknąć Dalej (Next).

Na kolejnych kartach należy zaznaczyć opcję CGI. FastCGI nie jest osobnym elementem, lecz modułem zawartym w najnowszej wersji CGI.

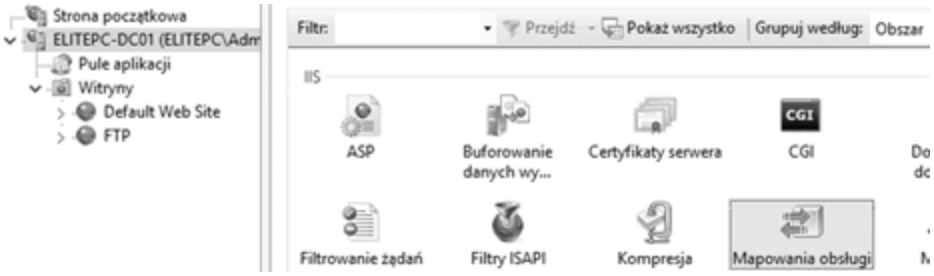
Należy także pobrać PHP ze strony PHP.net. Polecić można wersję non-thread-safe, ponieważ jest lepiej zoptymalizowana pod kątem wielowątkowości.

Należy rozpakować zawartość archiwum ZIP do katalogu PHP umieszczonego na dysku C.

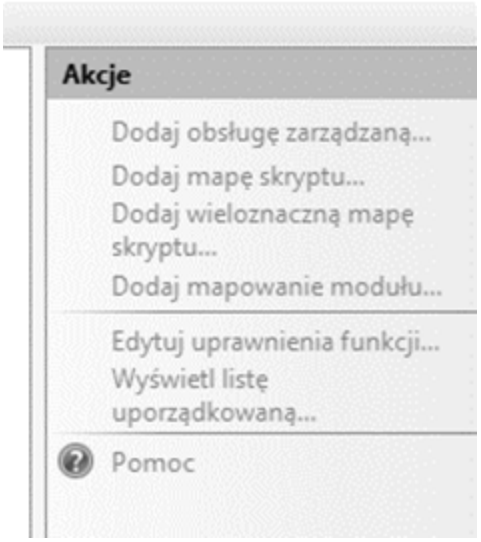


Następnie konieczna jest zmiana rozszerzenia pliku ze zdjęcia na *.ini

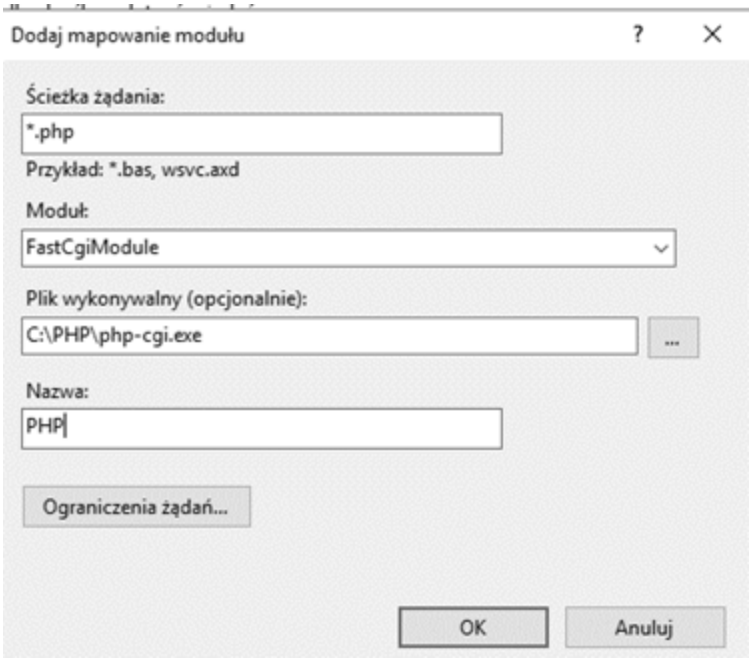
W Menadżerze IIS należy wybrać Mapowania Obsługi (Handler Mappings), przy zaznaczonym serwerze w menu po lewej stronie.



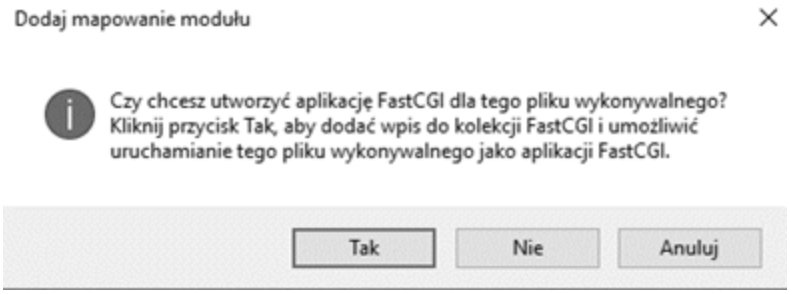
Następnie należy kliknąć w menu po prawej stronie w Dodaj mapowanie modułu (Add Module Mapping).



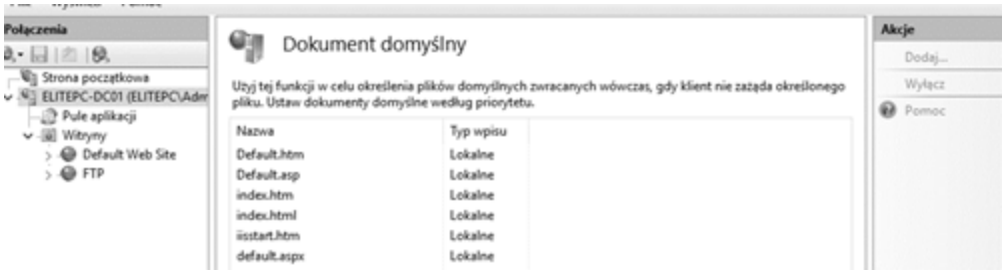
Planszę, która się pojawi, należy wypełnić tak, jak na poniższym zrzucie z ekranu:



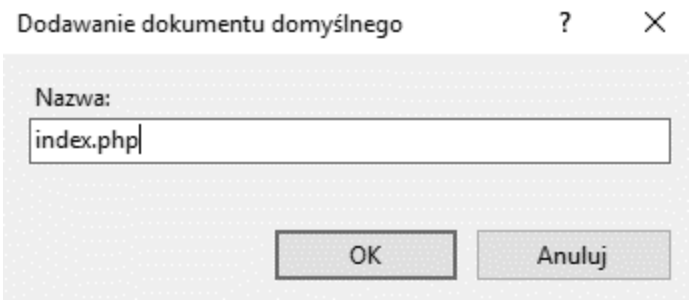
Należy kliknąć OK, a komunikat, który się pojawi potwierdzić przyciskiem Tak (Yes).



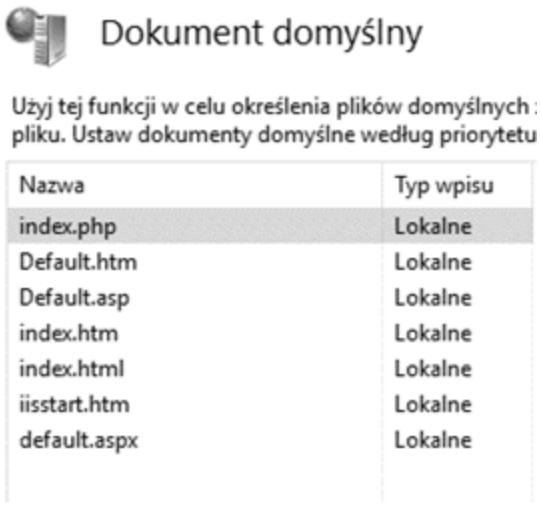
W menu po prawej stronie należy kliknąć Dodaj (Add…).



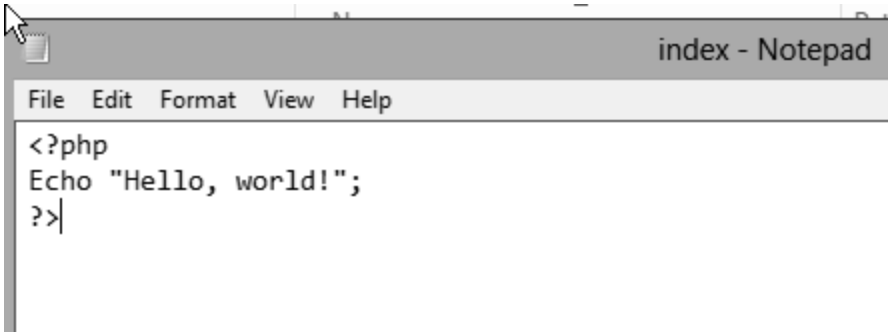
Aby strony napisane w języku PHP prawidłowo się wczytywały, należy także dodać domyślny dokument o nazwie index.php.



Gdy dokument zostanie już dopisany do listy, aby strona w języku PHP była wczytywana jako pierwsza, powinno się ustawić jej priorytet na najwyższy, umieszczając ją na szczycie listy domyślnych dokumentów.



Następnie należy otworzyć notatnik i zaimplementować bardzo prostą stronę www, a także zapisać ją w katalogu C:\inetpub\wwwroot\ jako index.php

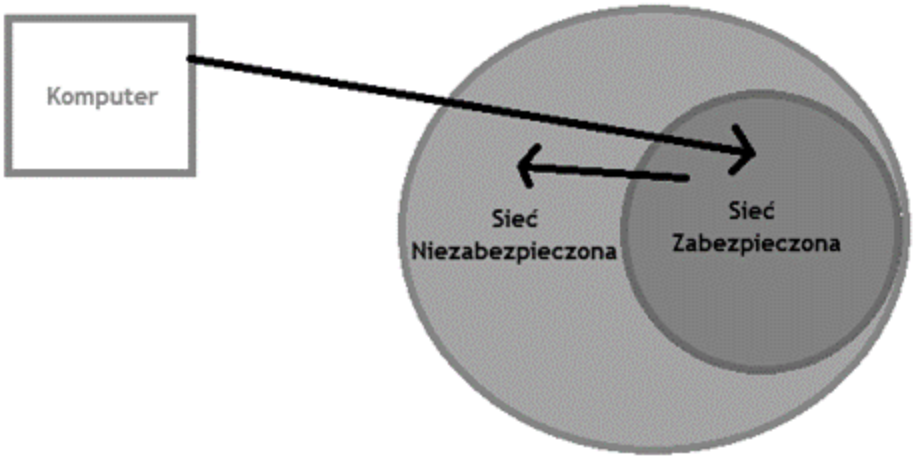


Na koniec trzeba zresetować serwer, a po jego ponownym rozruchu sprawdzić, czy strona działa.

7. Network Access Protection

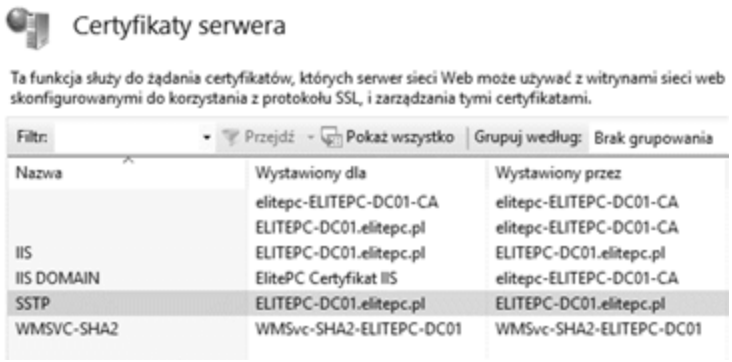
Jedną z nowości wprowadzonych do Windows Server 2008 był Network Access Protection (NAP), służący do zwiększenia bezpieczeństwa sieci. Pozwala on przeskanować zdalnie komputery i tym, które nie spełniają norm bezpieczeństwa, zabronić połączenia się z siecią. Schemat działania tego systemu przedstawia diagram poniżej. Ta sama funkcjonalność znajduje się także w Windows Server 2016.

7.1. Network Policy and Access Services



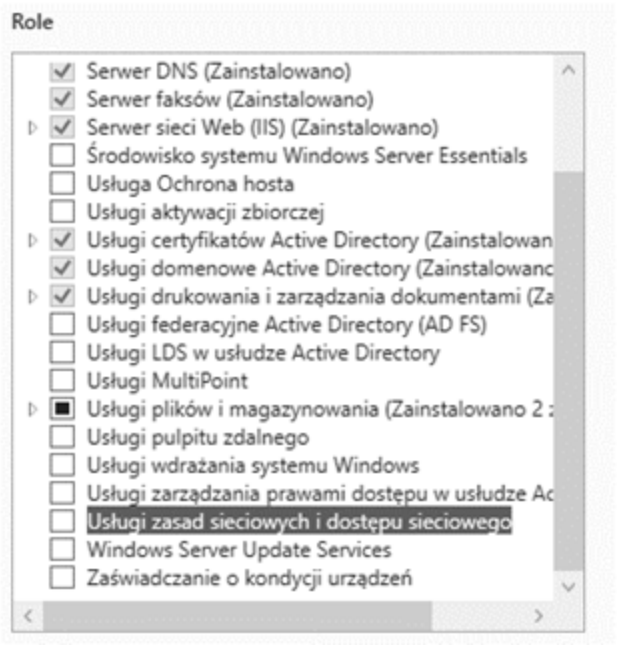
Zewnętrzny okrąg przedstawia niezabezpieczoną sieć firmową. Wewnętrzny natomiast pokazuje fragment sieci, w której działają tylko i wyłącznie komputery spełniające normy bezpieczeństwa. Maszyna spoza sieci, która próbuje uzyskać dostęp do zasobów, kontaktuje się z serwerem w sieci zabezpieczonej. Jeżeli spełniła ona warunki, czyli np. ma zainstalowany aktualny program antywirusowy oraz najnowsze aktualizacje bezpieczeństwa, przyłączenie komputera do sieci nie będzie stanowiło problemu. W przeciwnym wypadku maszyna zostanie przedelegowana do komputerów w sektorze niezabezpieczonym, gdzie będzie mogła uzyskać dostęp do witryny WWW z pomocą, czy też niezbędnych aktualizacji lub programów.

Należy skonfigurować taką polisę dla każdego rodzaju połączenia. W ramach tej publikacji posłużono się przykładem konfiguracji dla klientów DHCP. Uruchomiono także routing, aby komputery z sieci lokalnej miały dostęp do Internetu, jak również zapewniono zdalny dostęp do komputerów firmowych spoza siedziby za pośrednictwem bezpiecznego połączenia VPN.

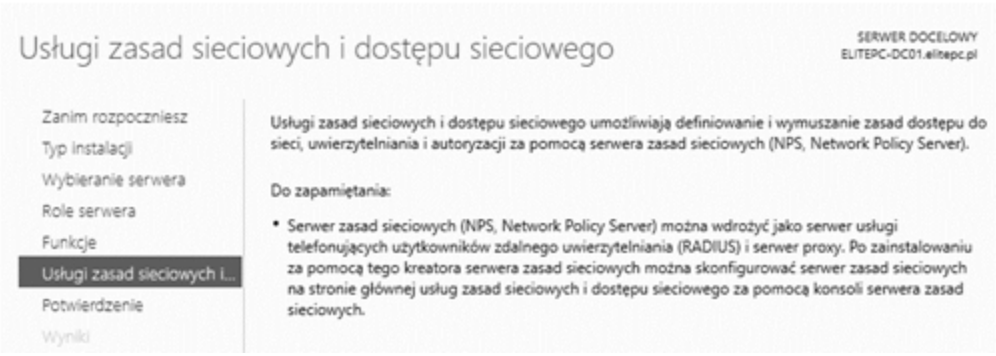


Później należy zainstalować rolę Usługi zasad i dostępu sieciowego (Network Policy and Access Services)

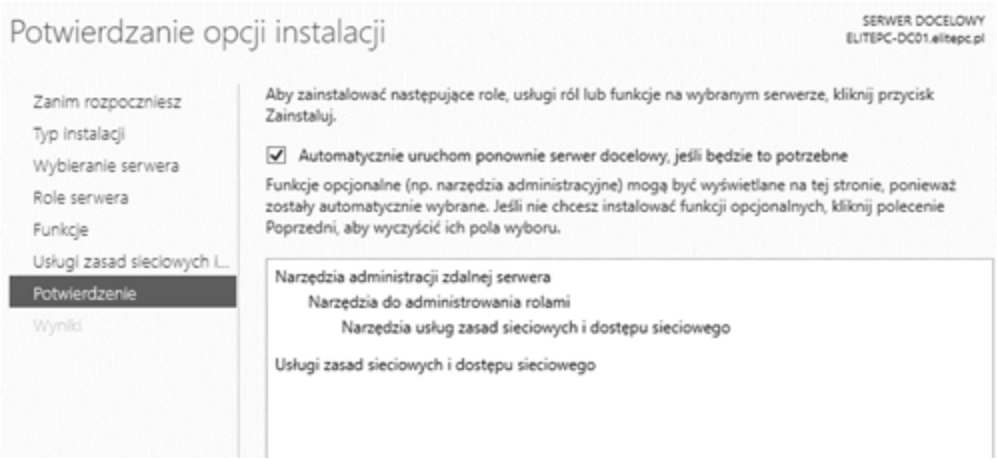
i zatwierdzić wybór kliknięciem w przycisk Dalej (Next).



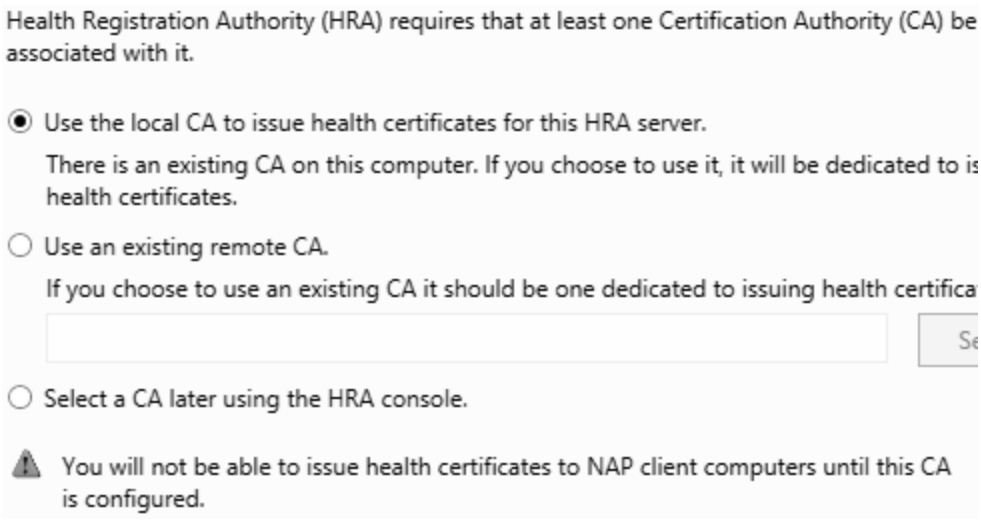
Na kolejnej planszy trzeba kliknąć Dalej (Next).



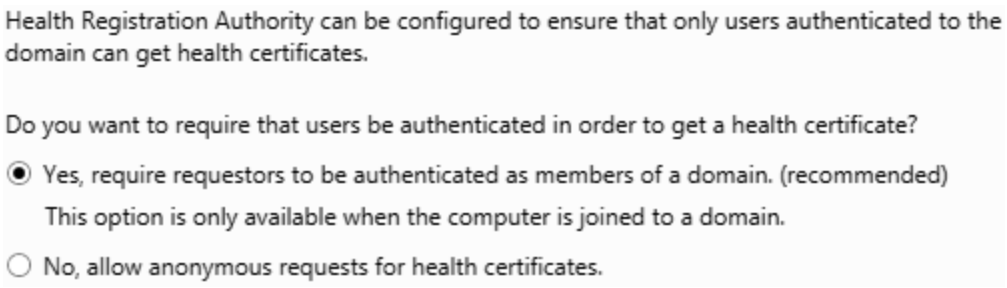
W ramach roli można zainstalować wszystkie usługi, ponieważ prędzej czy później okażą się one przydatne. Należy kliknąć Dalej (Next).



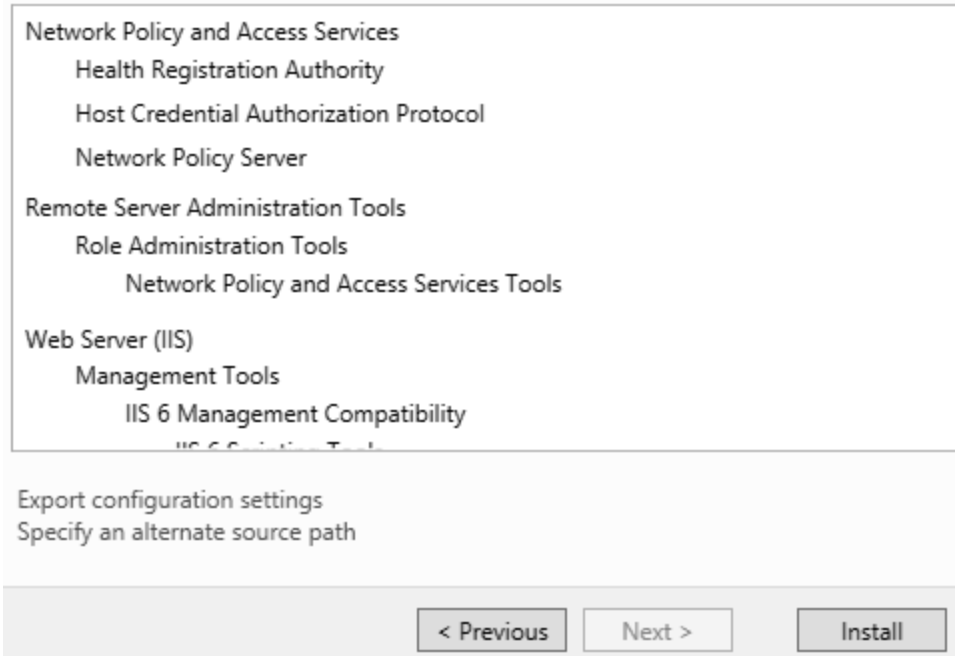
Jeżeli na komputerze nie ma jeszcze urzędu certyfikacji, teraz jest dobry moment, by go zainstalować. Jeżeli urząd już jest, należy wybrać go z listy. Można wybrać także opcję ze zrzutu ekranu, czyli skorzystanie z lokalnego CA.



Dla większego bezpieczeństwa powinno się wymagać, aby Użytkownicy uwierzytelniali się jako członkowie domeny (Yes, require requestors to be authenticated as members of a domain).

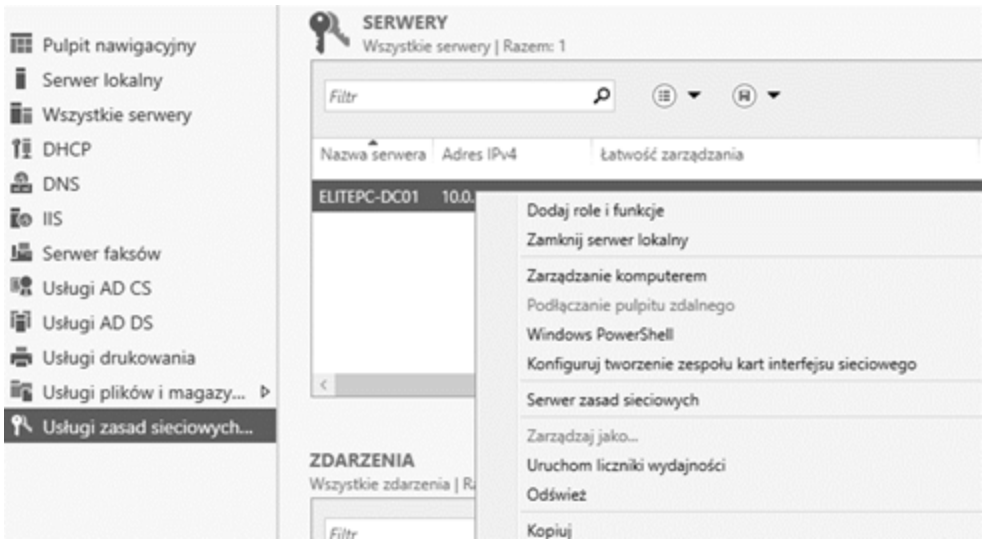


Na karcie podsumowującej należy kliknąć Zainstaluj (Install).

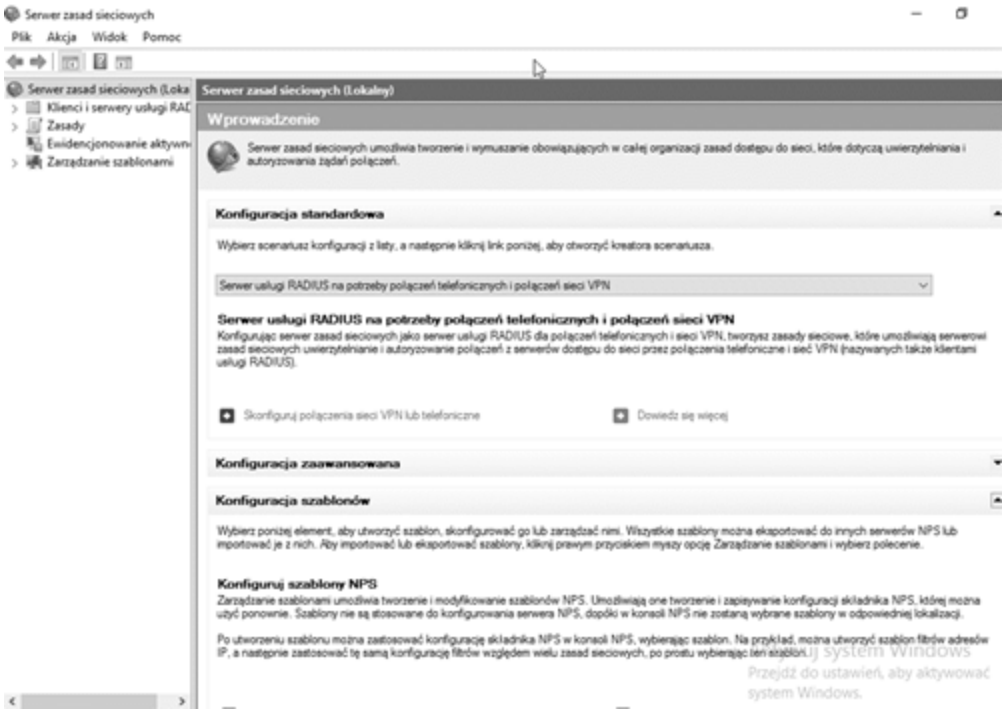


7.2. Zarządzanie Network Policy Server

W Menadżerze Serwera (Server Manager) znajduje się serwer zasad sieciowych NAP. Należy wybrać opcję Serwer Zasad Sieciowych (Network Policy Server), która wyświetli się po kliknięciuprawym przyciskiem myszy.



Po jego uruchomieniu można skorzystać z gotowych kreatorów.



8. VPN, Direct Access i NAT

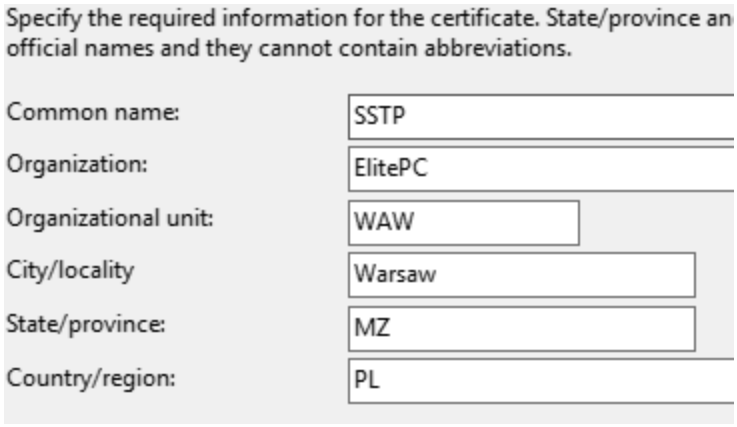
Funkcje VPN i Direct Access zapewniają użytkownikowi spoza domeny swobodną pracę z wykorzystaniem zasobów wewnątrz firmy. Z kolei NAT uruchamia translację adresów sieciowych, czyli w przypadku, gdy bramką sieciową jest Windows Server, NAT pozwala na połączenie komputerów wewnątrz sieci z siecią zewnętrzną.

8.1. Instalacja roli Remote Access

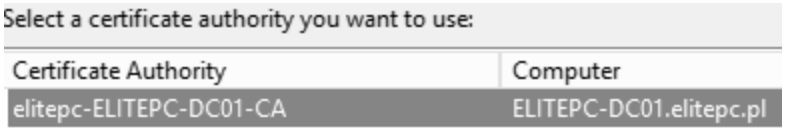
Zostanie teraz skonfigurowane połączenie VPN typu SSTP, czyli szyfrowane z certyfikatem, które jest znacznie bezpieczniejsze od PPTP. Pierwszym najważniejszym krokiem będzie więc zainstalowanie certyfikatu. Bardzo ważnym jest, aby zrobić to przed instalacją Routingu. W przeciwnym wypadku nie osiągnie się celu. Wymagana będzie instalacja wcześniej roli IIS. Aby tego dokonać, należy wejść do Menadżera IIS i kliknąć dwukrotnie w Certyfikaty Serwera (Server Certificates).

Następnie należy wybrać opcję Utwórz Certyfikat Domeny. Pojawi się kreator, w którym pierwszą planszę

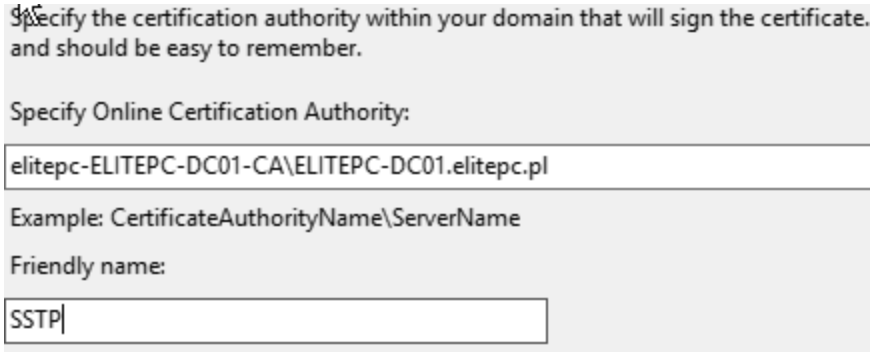
trzeba wypełnić wedle uznania, gdyż są to tylko nieznaczące informacje, i wcisnąć przycisk Dalej (Next).



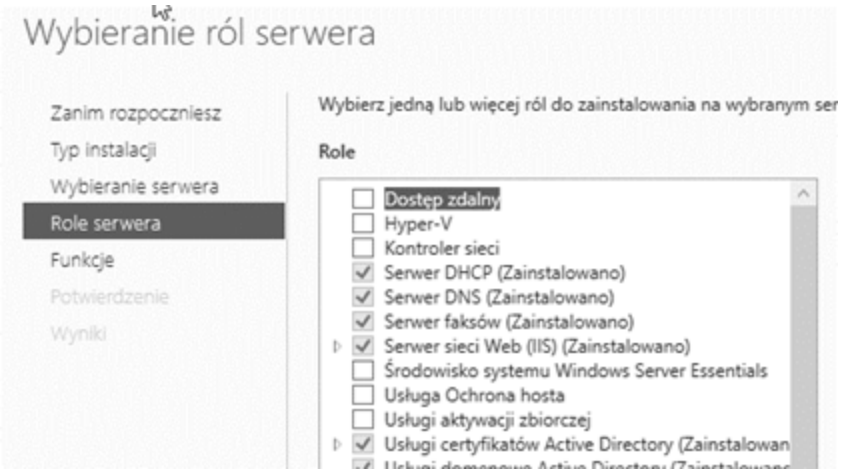
Na kolejnej planszy należy kliknąć przycisk Wybierz (Choose) i z listy wybrać serwer, na którym zainstalowany jest główny urząd certyfikacji.



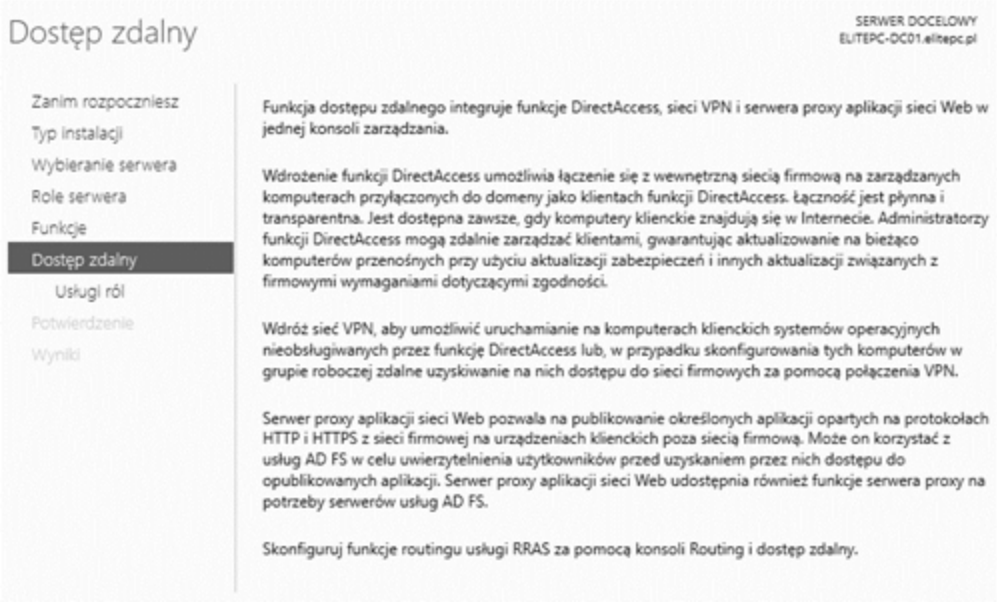
Należy nazwać wprowadzony certyfikat, dlatego powinno się wypełnić pole dotyczące jego Przyjaznej nazwy (Friendly name), a następnie kliknąć przycisk Zakończ (Finish).



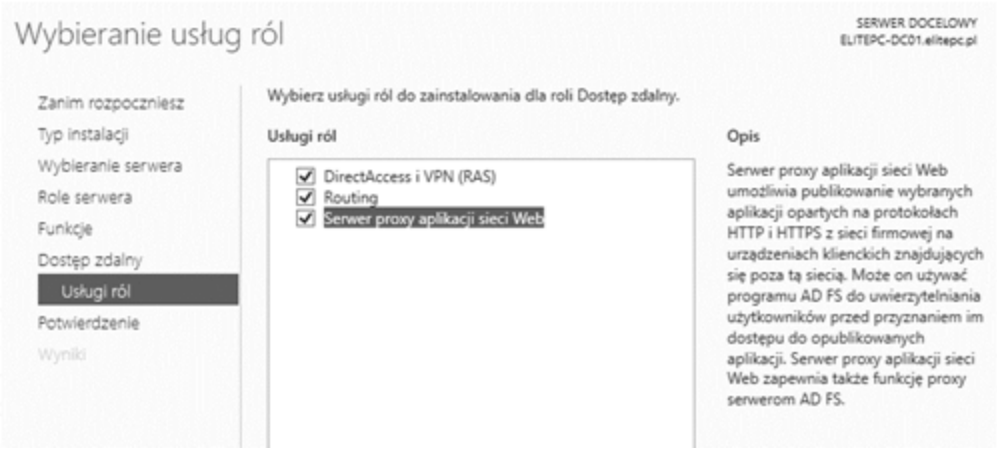
Certyfikat pojawi się na liście. Można teraz przystąpić do instalacji. W Menadżerze Serwera (Server Manager) należy dodać rolę Zdalny Dostęp (Remote Access).



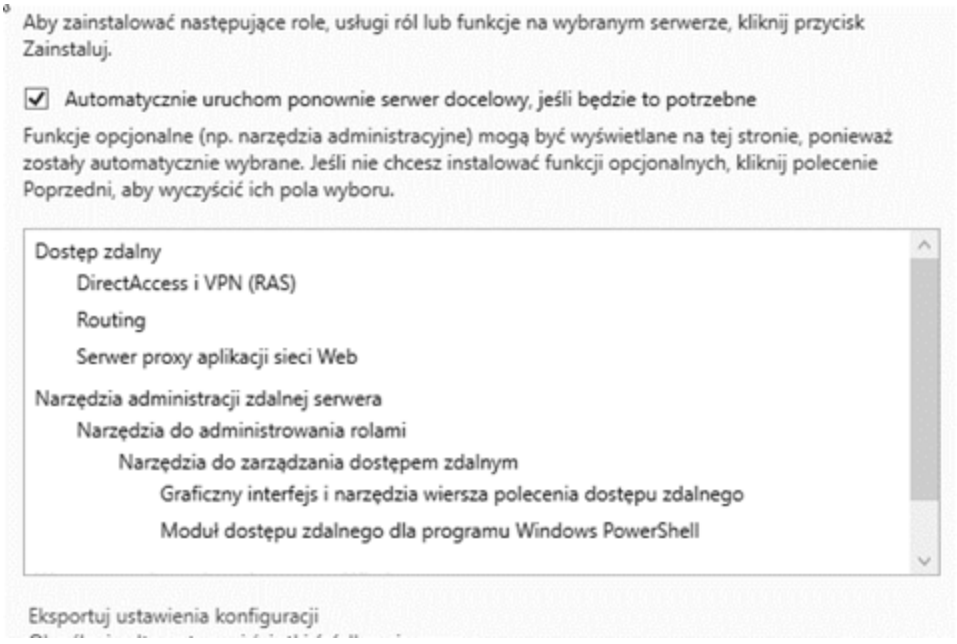
Należy pamiętać o tym, iż w przypadku Windows Server, VPN jest nierozerwalny z Routingiem (RRAS). W Windows Server 2008 usługi, które są omawiane, były włączone do roli NAP, w Windows Server 2016 zostały rozdzielone. W czasie instalacji konieczne jest kliknięcie przycisku Dalej (Next) na karcie powitalnej.



W kolejnym oknie można zainstalować DirectAcces i VPN, które są ze sobą połączone, jak również Routing, dzięki któremu będzie możliwe udostępnienie Internetu stacjom klienckim poprzez protokół IPv4.



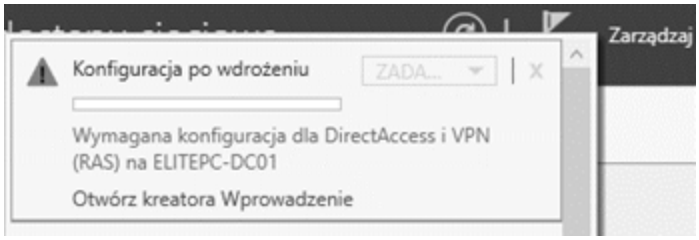
Warto więc wybrać wszystkie opcje. Wymagane będą także pojedyncze komponenty serwera IIS, które należy zainstalować, jeżeli to wcześniej nie zostało wykonane. Jeżeli natomiast jest już zainstalowany IIS, to można przejść od razu do podsumowania i kliknąć Zainstaluj (Install).



8.2. Konfiguracja VPN i NAT

Po zakończeniu instalacji należy z poziomu Centrum akcji (Action Center) uruchomić konfigurację zainstalowanej roli.

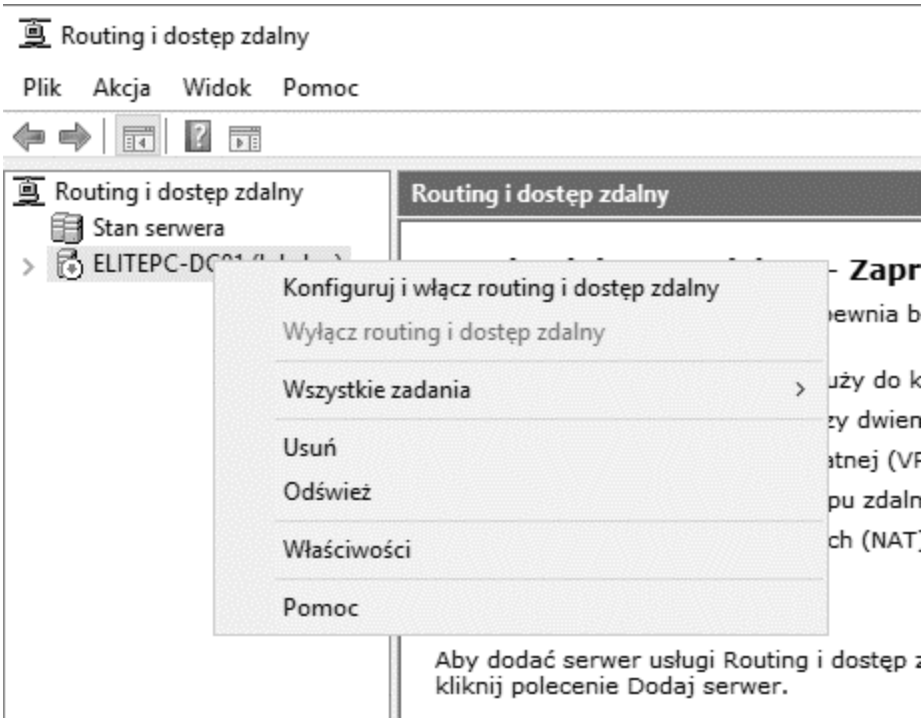
.



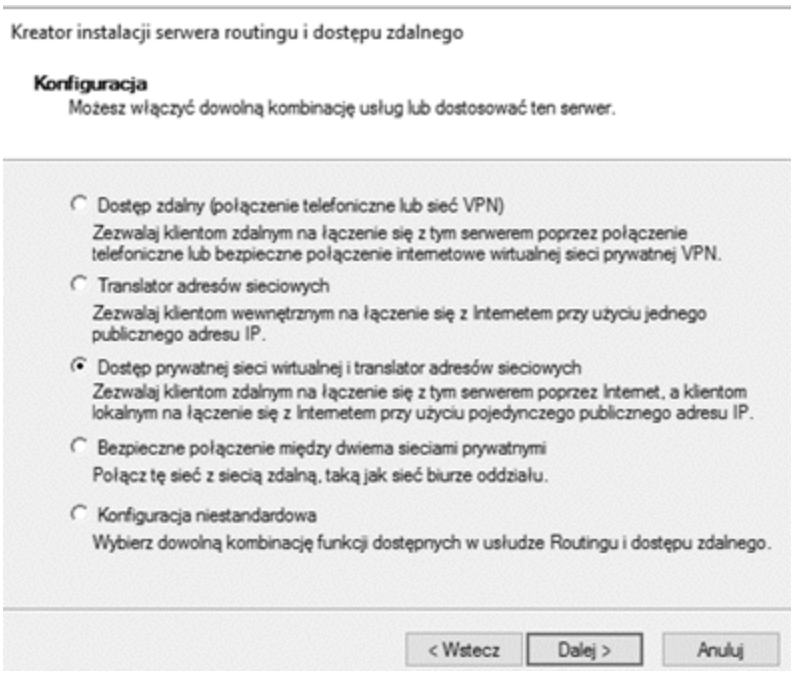
Do wyboru są trzy opcje. Konfiguracja serwera VPN i Direct Access jednocześnie, bądź jedynie wybranego z nich. W przykładzie zostanie skonfigurowany na razie tylko VPN, ponieważ jest to proces analogiczny względem wcześniejszych wersji sytemu Windows Server.

Po wybraniu trzeciej opcji pojawi się znana administratorom z Windows Server 2003, 2008 i 2012 konsola Routing i dostęp zdalny (Routing and Remote Access).

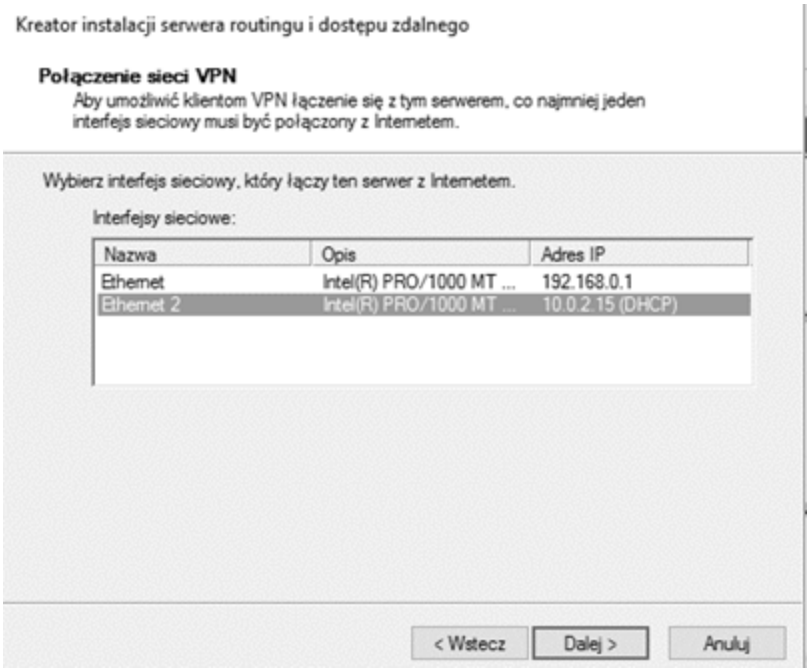
Należy kliknąć prawym przyciskiem myszy na nazwie komputera i wybrać opcję Konfiguruj i Włącz Routing i Dostęp Zdalny (Configure and Enable Routing and Remote Access).



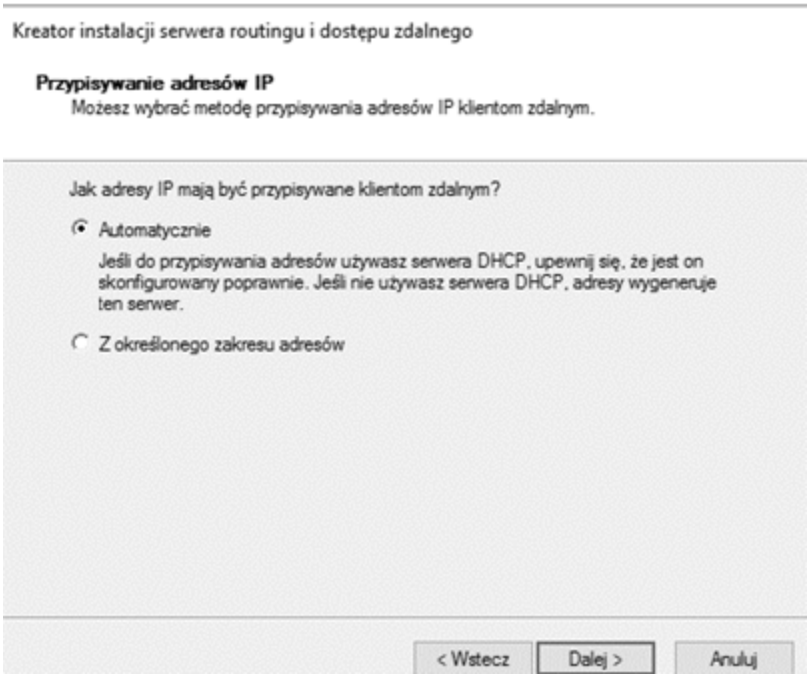
Następnie należy kliknąć Dostęp prywatnej sieci wirtualnej i translator adresów sieciowych (Virtual private network (VPN) access and NAT), a potem wybrać przycisk Dalej (Next).



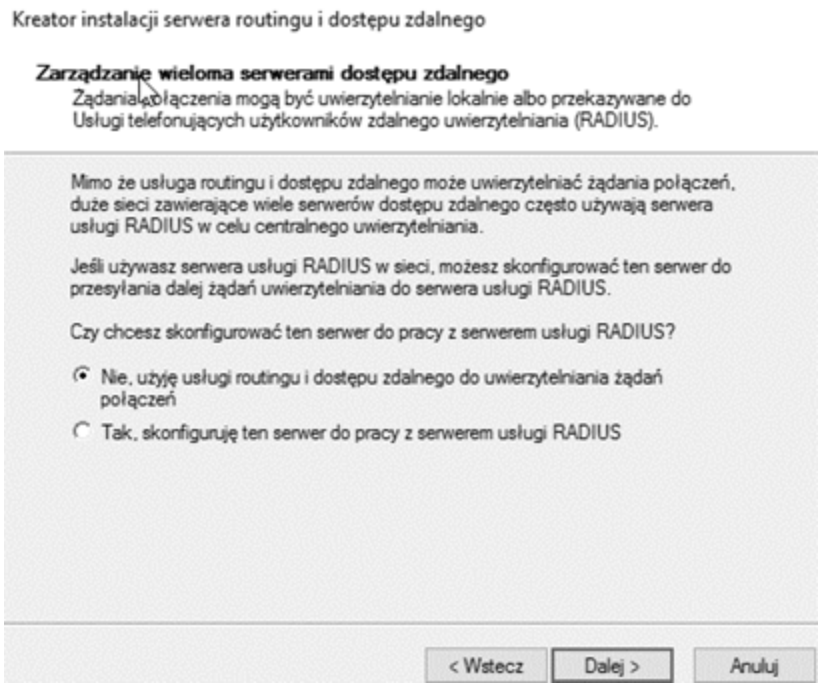
W kolejnym kroku należy wybrać interfejs sieciowy, który będzie łączył z Internetem.



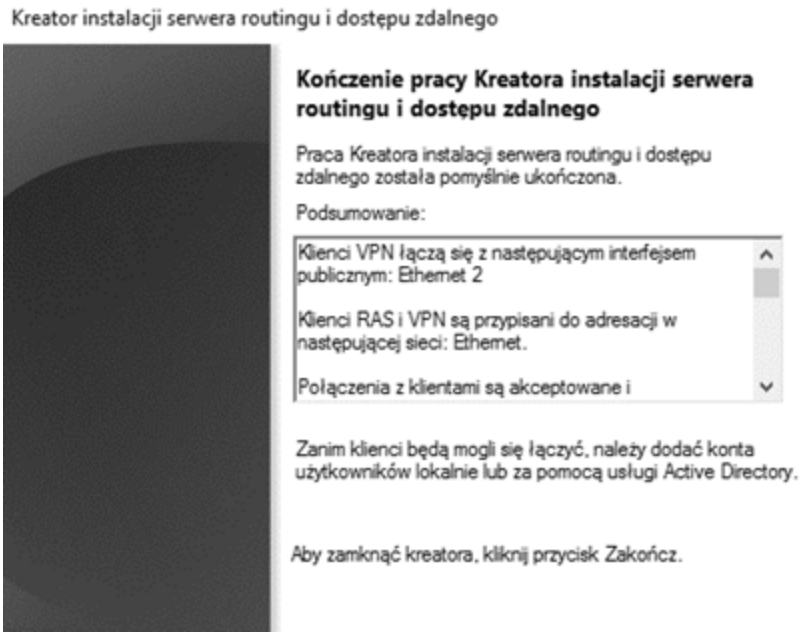
Jeśli chodzi o przypisywanie adresów, można wybrać Automatyczne (Automatically), ponieważ w sieci jest już skonfigurowany serwer DHCP, więc nie ma konieczności używania serwera DHCP wbudowanego w RRAS.



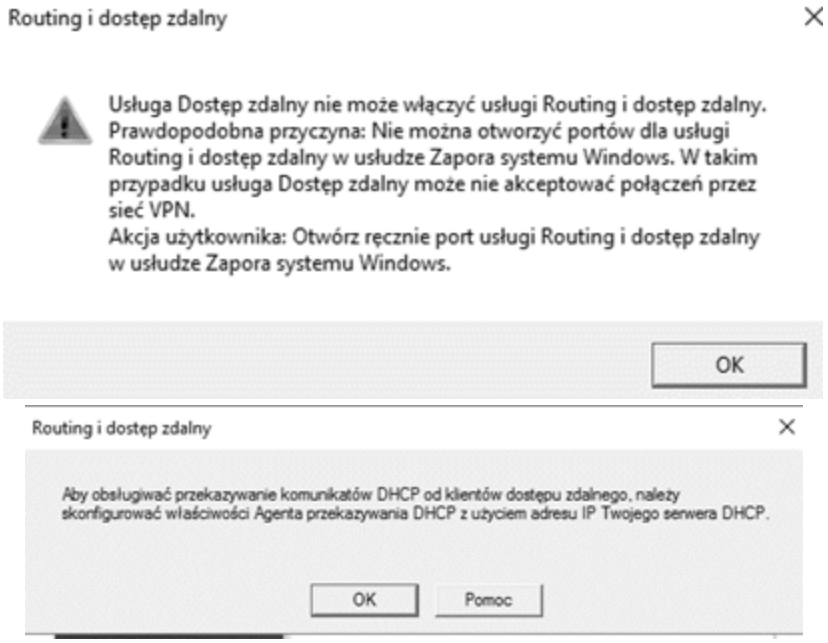
W sieci testowej nie ma serwera Radius, dlatego też należy wybrać opcję pierwszą.



Na karcie z podsumowaniem należy wybrać Zakończ (Finish).

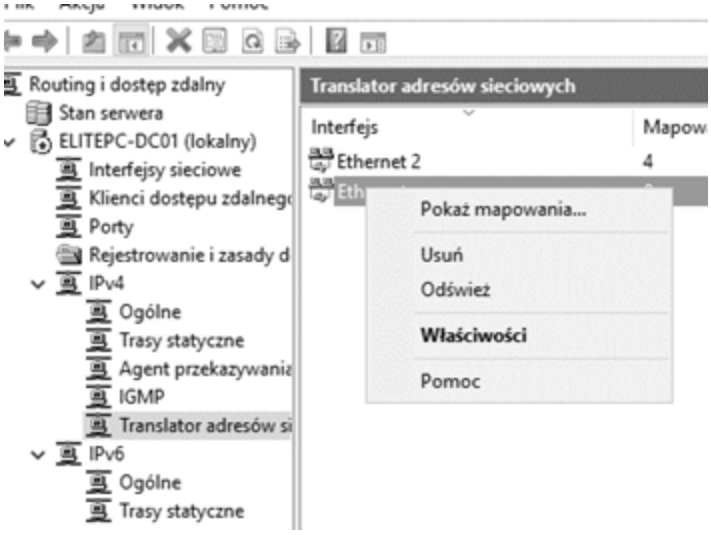


Pojawią się dwa komunikaty. Oba należy zatwierdzić przyciskiem OK.

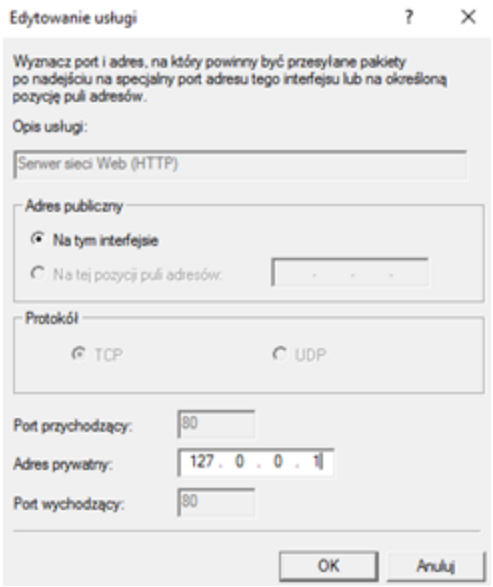


Po chwili oczekiwania, jeżeli wszystko się powiedzie, w sekcji Porty (Ports) zostaną utworzone mini porty SSTP.

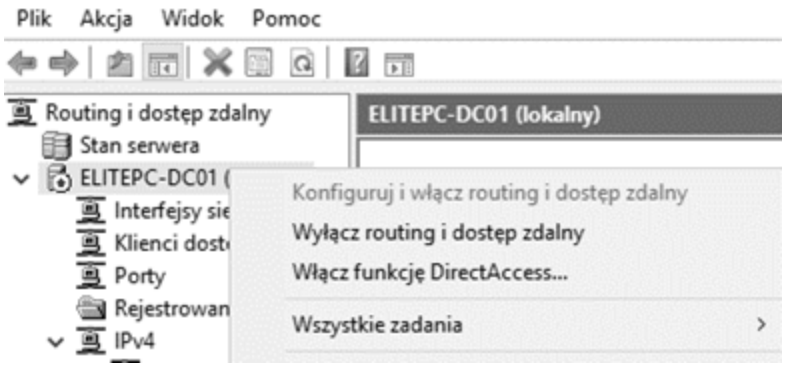
Konieczne jest jeszcze odblokowanie w Zaporze Systemowej (Firewallu) portu 80, aby klienci mogli odbierać certyfikat. Na połączeniu WAN należy więc kliknąć prawym klawiszem myszy i wybrać Właściwości (Properties).



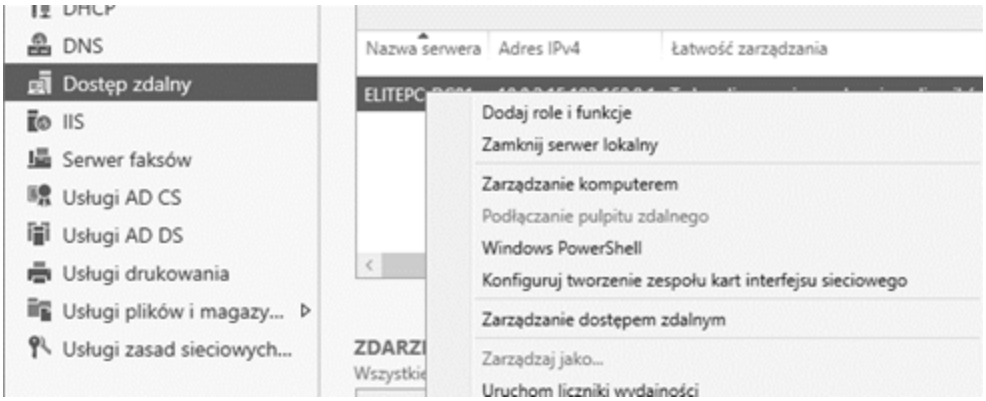
Następnie należy wejść w zakładkę Usługi i Porty (Services and Ports) i zaznaczyć Serwer WWW (Web Server), a jako adres prywatny podać Localhost i kliknąć OK.



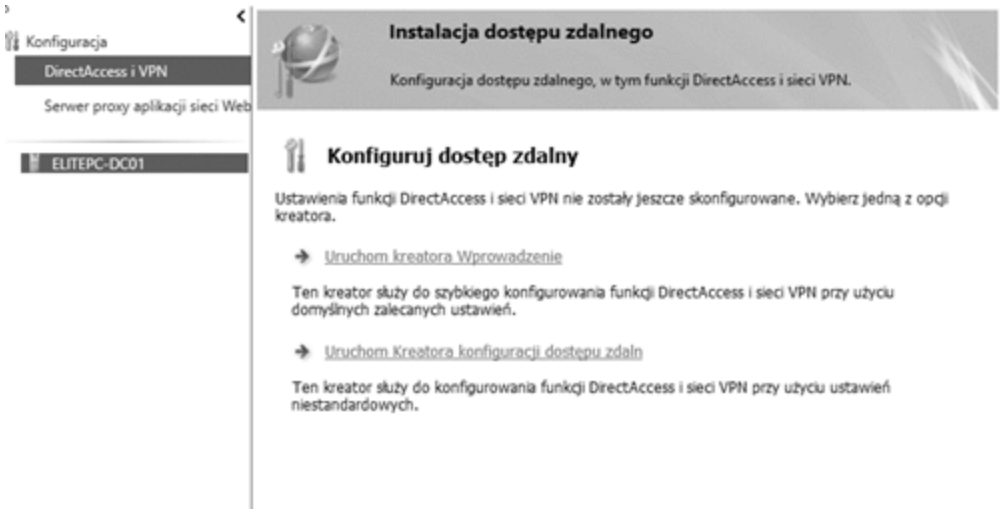
Nowością względem starszych wersji systemu Windows Serwer jest przycisk umożliwiający uruchomienie Zdalnego Dostępu (Direct Access) z poziomu menu kontekstowego serwera RRAS.



Warto teraz zajrzeć do Menadżera Serwera (Server Manager), gdzie również pojawił się Zdalny Dostęp (Remote Access). Po wybraniu serwera istnieje możliwość uruchomienia konsoli Menadżer Zdalnego Dostępu (Remote Access Management).



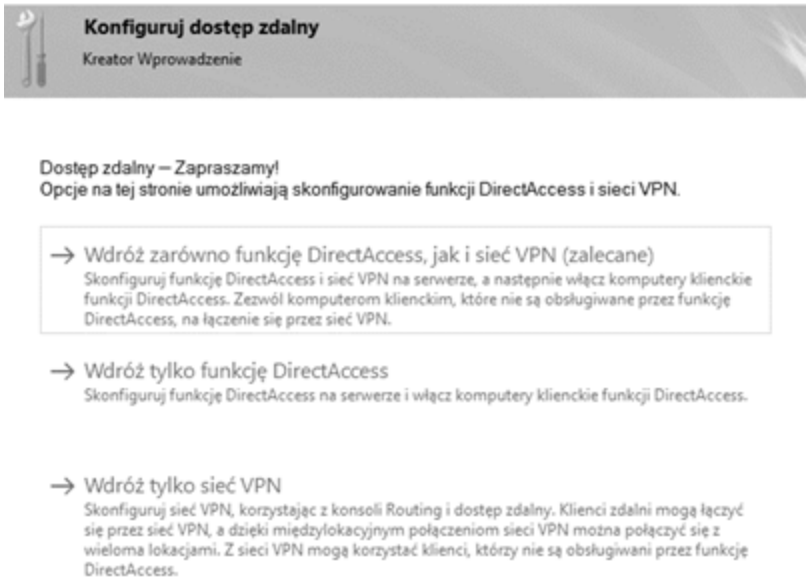
W sekcji Konfiguracja (Configuration) znajduje się schemat przedstawiający działanie roli.



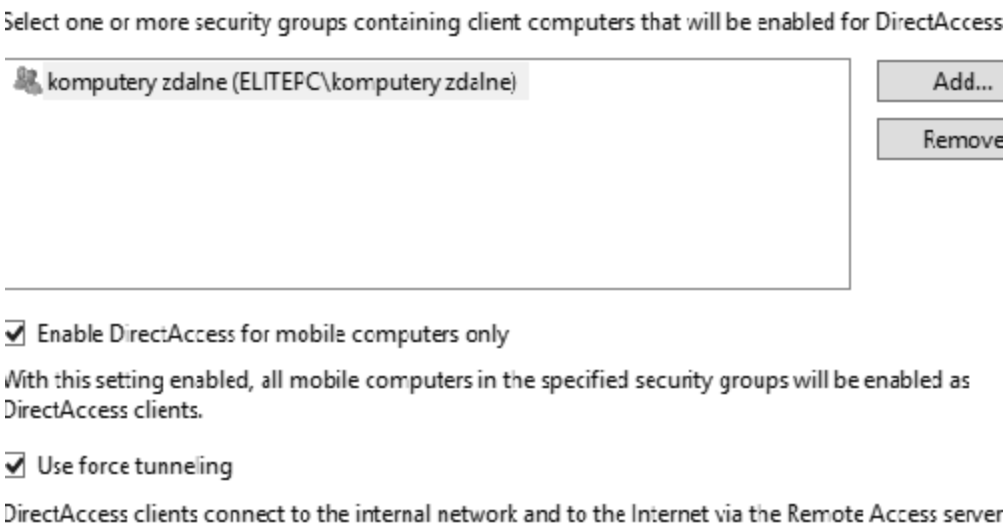
8.3. Konfiguracja DirectAccess

Należy pamiętać, że DirectAccess wymaga IPv6 wprowadzonego i działającego globalnie, a więc jest to funkcja raczej przyszłościowa. Dzięki tej technologii użytkownicy zdalni będą zawsze mieli dostęp do wewnętrznej sieci firmowej, bez potrzeby nawiązywania połączenia VPN. Co więcej, taki zdalny użytkownik jest cały

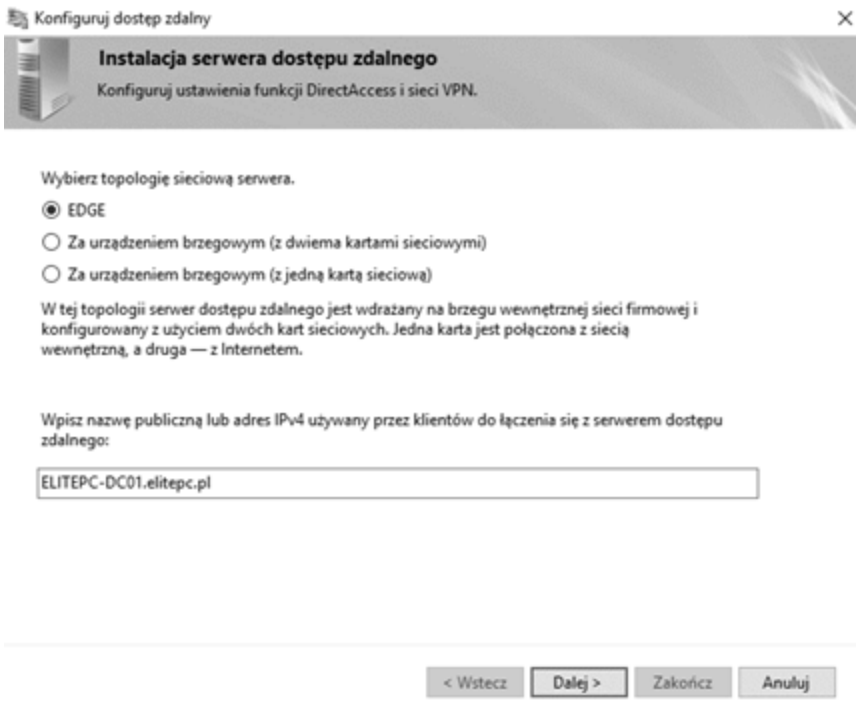
czas podłączony do sieci firmowej, nawet przed zalogowaniem się na własne konto użytkownika, jedyny wymóg to połączenie z Internetem. Z kolei administrator sieci może takim komputerem zarządzać na odległość, tak samo jakby był on wpięty do sieci. Cała komunikacja odbywa się w sposób bezpieczny po IPSec. W celu ćwiczeniowym należy więc wcisnąć przycisk Uruchom kreatora, aby zobaczyć ekran powitalny, który między innymi informuje o tym, że DirectAccess może spokojnie działać „obok” VPN.



Po kliknięciu przycisku Dalej (Next) kreator sprawdzi, czy komputer spełnia wszelkie wymagania, jeżeli tak, to przejdzie do karty, na której trzeba określić, które grupy komputerów z usługi katalogowej mają mieć dostęp przez DirectAccess. Ponadto można tu przefiltrować wybrane grupy tak, aby tylko maszyny mobilne miały dostęp przez DA, a także wymusić tunelowanie połączenia.

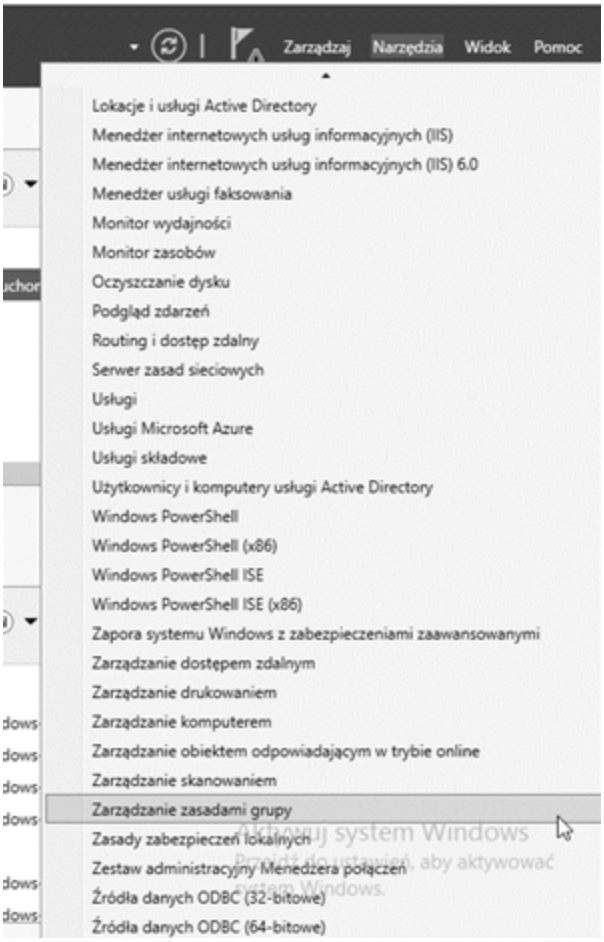


Kolejnym krokiem jest określenie topologii sieci serwera. Edge to topologia, gdzie serwer dostępu zdalnego stoi na pograniczu sieci zewnętrznej i sieci wewnętrznej, na ogół posiada dwa lub więcej adapterów sieciowych, gdzie jeden łączy z Internetem, a drugi z siecią firmową. Drugi rodzaj – Behind an Edge device – występuje w wersji posiadającej jedną lub dwie karty sieciowe. Scenariusz z dwiema kartami sieciowymi zakłada, że klientów spoza sieci oraz serwer dzieli jeszcze jakieś inne urządzenie, jak np. firewall, do którego wpięty jest serwer, podczas gdy druga karta komunikuje się z siecią wewnętrzną. Ostatni scenariusz z jedną kartą sieciową zakłada, że serwer nie pełni roli bramki, tylko jest po prostu wpięty bezpośrednio do sieci firmowej.

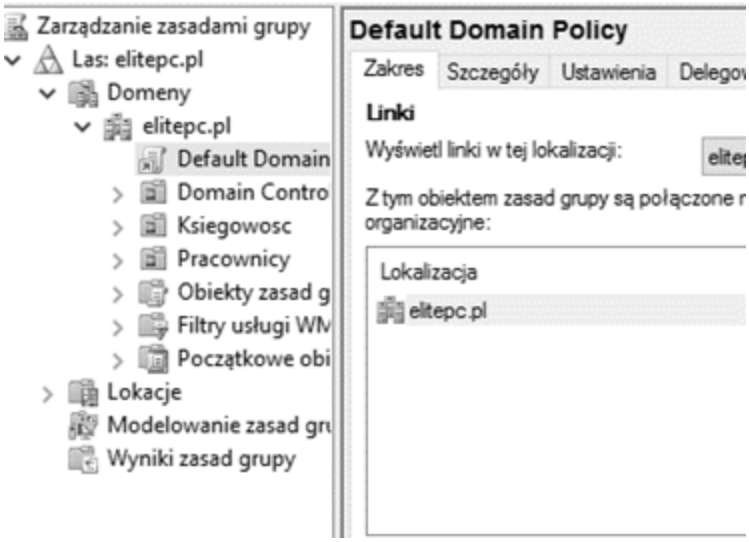


9. Polisy (Zarządzanie Zasadami Grupy)

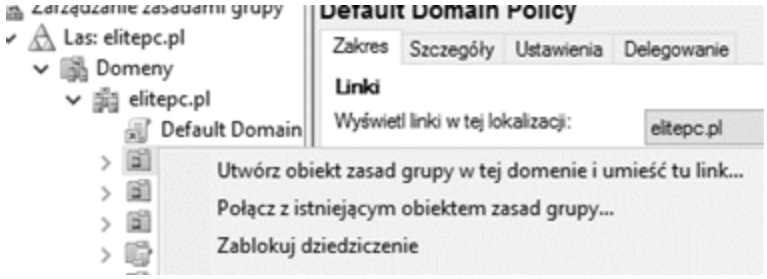
Polisy pozwalają na scentralizowane zarządzanie i konfigurowanie praktycznie całego systemu. Innymi słowy, pozwalają na kontrolowanie tego, co użytkownicy mogą robić, a czego nie. Administrator może swobodnie kontrolować funkcje dostępne użytkownikom, nawet zabronić im takich drobnostek jak zmiana tapety. Aby wejść do konsoli Zarządzania Zasadami Grupy (Group Policy Management), należy kliknąć z poziomu Menadżera Serwera (Server Manager) w guzik Narzędzia (Tools), a następnie wybrać Zarządzanie Zasadami Grupy (Group Policy Managament).



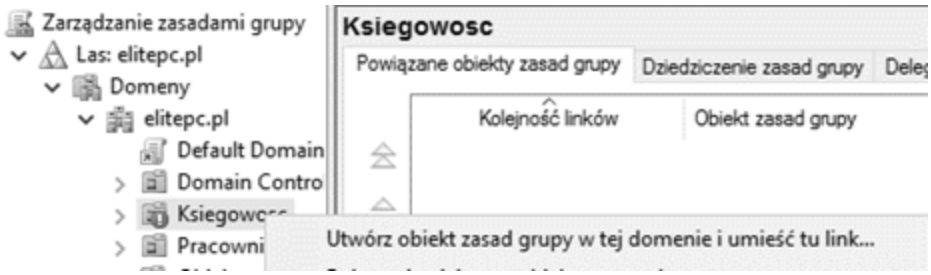
Po rozwinięciu drzewa z lewej strony, można dostrzec tam domenę, a także utworzone wcześniej jednostki organizacyjne. Jest też Domyślna polisa domeny (Default Domain Policy), co – jak nazwa wskazuje – jest domyślną polisą dla domeny. Wszystko, co znajduje się w drzewie pod nią, dziedziczy po niej, czyli, mówiąc krótko, korzysta z niej. Ponieważ we wcześniejszych rozdziałach był konfigurowany DirectAccess, również i dla tej roli pojawiły się dwie polisy. Gdyby DirectAccess nie był zainstalowany, nie byłoby ich tu (DirectAccess Client Settings oraz DirectAccess Server Settings).



Jeżeli zajdzie taka potrzeba, dziedziczenie można zawsze wyłączyć poprzez kliknięcie prawym przyciskiem w odpowiednią jednostkę organizacyjną i wybranie opcji Zablokuj dziedziczenie (Block Inheritence).

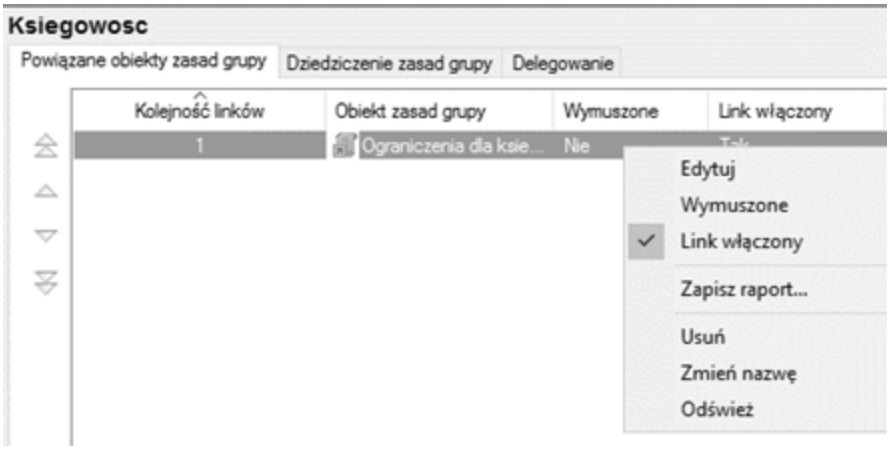


W tym przypadku jednak nie ma takiej potrzeby. W celach ćwiczeniowych zostanie stworzona nowa polisa dla Księgowości. W tym celu należy kliknąć ponownie prawym przyciskiem i wybrać opcję Utwórz obiekt zasad grupy w tej domenie i umieść tu łącze (Create a GPO in this domain, and Link it here). Warto też zwrócić uwagę, że jeżeli już wcześniej została stworzona polisa, która by spełniała odpowiednie wymagania, można ją podłączyć, wybierając Połącz z istniejącym obiektem zasad grupy (Link an Existing GPO).



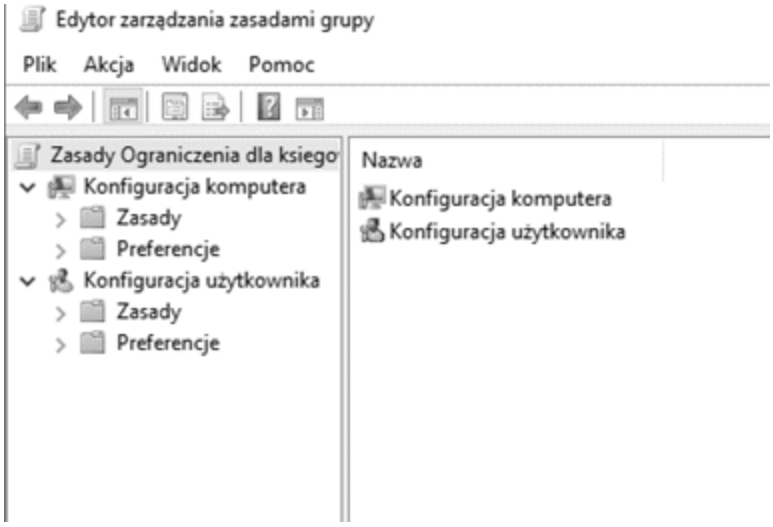
Pojawi się ekran, w którym należy podać nazwę dla nowej polisy. Dobrze, aby była ona intuicyjna, np. Ograniczenia dla Księgowości, i zatwierdzić wybór przyciskiem OK.

Po wybraniu kontenera Księgowość pojawi się ona na liście po prawej stronie okienka i w drzewie pod kontenerem. Jeżeli ma być ona zawsze wymuszona, należy kliknąć w nią prawym przyciskiem myszy i zaznaczyć opcję Wymuszone (Enforced), a następnie zatwierdzić wybór, klikając OK. Dzięki temu, mimo że wybrana polisa jest niżej w hierarchii, będzie ważniejsza.



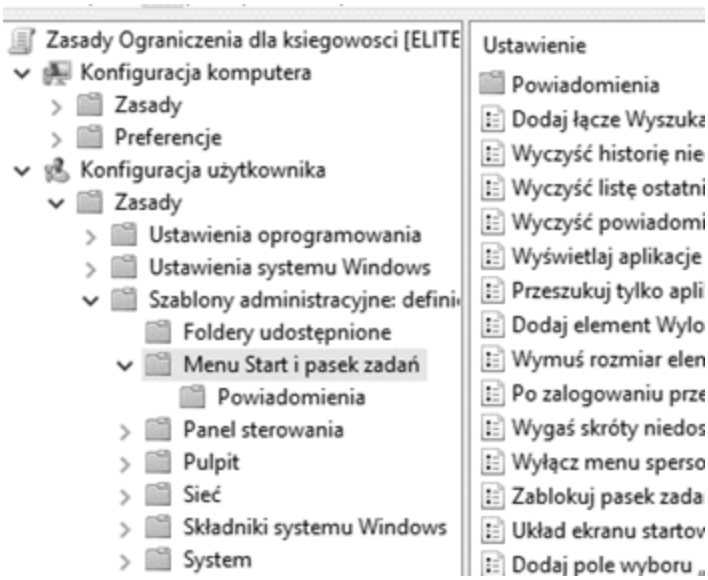
Teraz nadszedł czas na podjęcie decyzji, co ta polisa ma robić. Po raz kolejny należy kliknąć w nią prawym przyciskiem myszy, wybierając opcję Edytuj (Edit).

Otworzy się Edytor zarządzania zasadami grupy (Group Policy Management Console). W książce zostanie jednak pominięta informacja, do czego służy jaka zasada i gdzie się ona znajduje. Jest to narzędzie na tyle intuicyjne, że wystarczy przeczytać opisy pojedynczych opcji, aby zorientować się bez problemu, co dana zasada robi. Niemniej, przy odrobinie cierpliwości uda się odnaleźć odpowiednie elementy i skutecznie ograniczyć użytkowników.

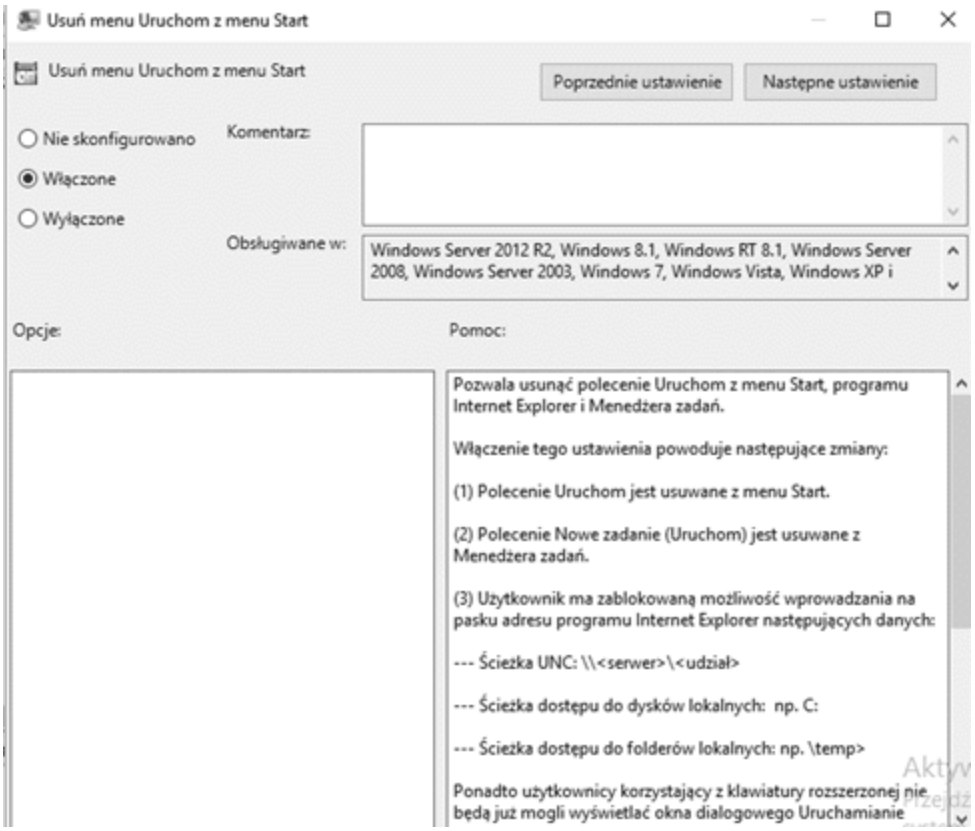


W celach ćwiczeniowych można trochę odchudzić za pomocą polis menu Start. Aby tego dokonać, należy rozwinąć listę w następujący sposób: Konfiguracja użytkownika > Zasady > Szablony administracyjne > Menu

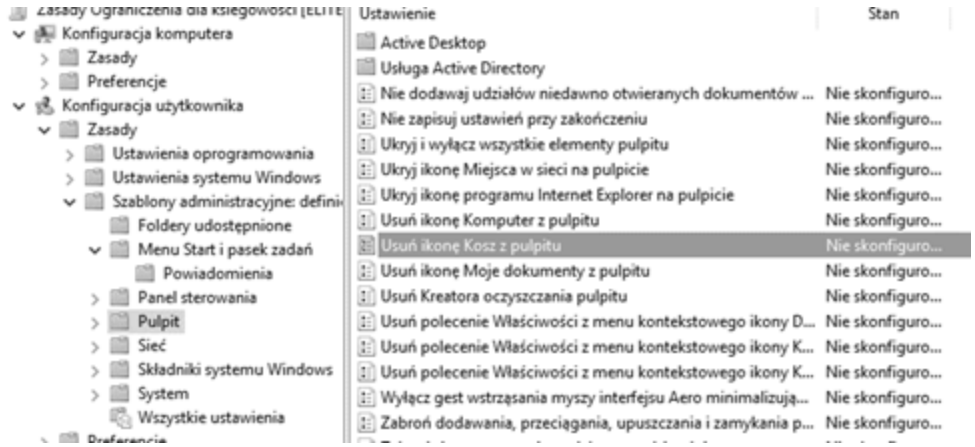
Start i pasek zadań (Computer Configuration > Policies > Administrative Templates > Start Menu and Taskbar).



Następnie należy dwukrotnie kliknąć w Usuń menu Pomoc z menu Start (Remove Search Link from Start Menu). W oknie, które się pokaże, należy zaznaczyć opcję Włączone (Enabled), a potem Zastosuj (Apply) i potwierdzić wybór przyciskiem OK. Tak samo można zrobić dla opcji Usuń menu Uruchom z menu Start (Remove Run Menu from Start Menu). Można jeszcze dla przykładu wyłączyć opcję Wyloguj z menu Start (Remove Logoff on the Start Menu).



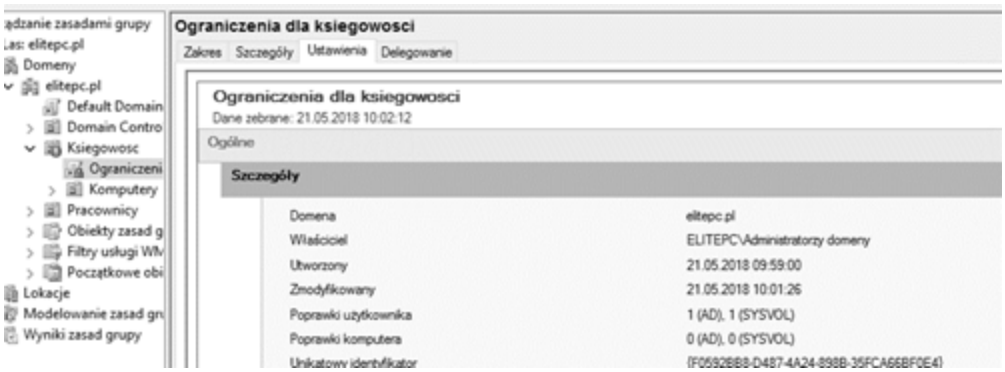
W sekcji Pulpit (Desktop) można uruchomić opcję Usuń ikonę Kosz z pulpitu (Remove Recycle Bin icon from desktop).



Dzięki takim poczynaniom użytkownik straci dostęp do pomocy, nie będzie mógł korzystać z opcji „uruchom”, a także już nigdy nie zostawi włączonego komputera w pracy, bo, aby się wylogować, będzie musiał wyłączyć

komputer. Kiedy dokonywanie zmian zostanie ukończone, należy kliknąć Plik (File) i wybrać opcję Zakończ (Finish). Zostanie ona zastosowana do wszystkich maszyn i użytkowników znajdujących się we wnętrzu kontenera Księgowość.

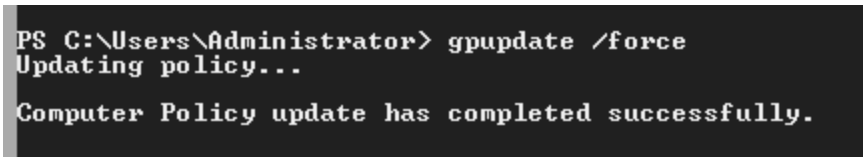
Warto zauważyć, że stworzona chwilę temu polisa została dodana tuż obok napisu Księgowość w GPO. Po kliknięciu na nią, a następnie po wybraniu Ustawień (Settings) z zakładek po prawej stronie, pojawi się dość intuicyjny wgląd do zmian, jakie dana polisa wprowadza.



Aby sprawdzić, czy powyższe zabiegi odniosły jakikolwiek skutek, należy zalogować się na komputerze klienta, w tym przypadku można zalogować się np. jako Kasjer. W następnej kolejności należy uruchomić konsolę CMD lub PowerShell, a w niej wpisać polecenie „gpupdate /force”, które spowoduje pobranie z kontrolera domeny najnowszych polis bezpieczeństwa oraz ich zastosowanie. Można to samo osiągnąć, po prostu uruchamiając komputer ponownie. Co więcej, odświeżenie polis przez automat nie zawsze poskutkuje od razu, dlatego warto je wymusić.

Odświeżanie zasad bezpieczeństwa chwilę potrwa, lecz jeżeli wszystko zostało prawidłowo skonfigurowane,

zakończy się sukcesem.

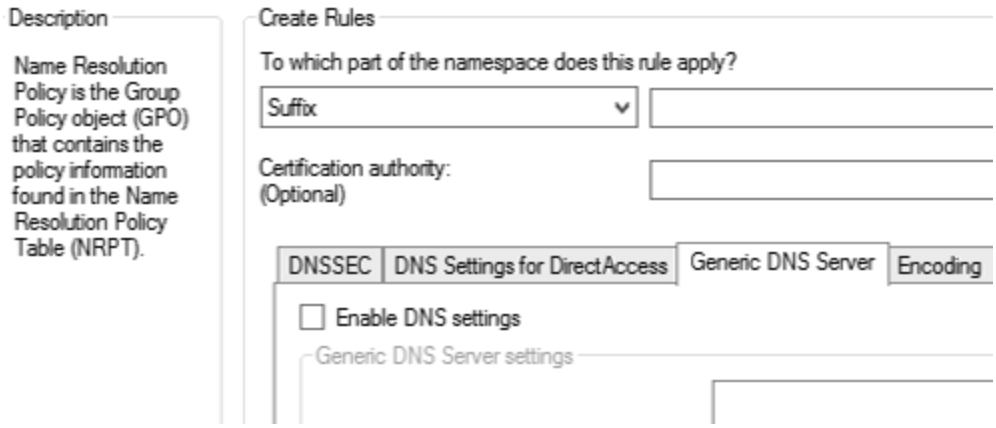


Podsumowując, polisy stanowią bardzo potężne narzędzie w rękach administratora. Używa się ich nie tylko do dostosowywania takich banałów jak te przedstawione w przykładzie, ale przede wszystkim do zabezpieczania komputera. Na przykład można blokować różne kombinacje klawiszy, strony internetowe, dołączać lokacje sieciowe, można zablokować możliwość instalowania różnych aplikacji, korzystania z gier itp. Bez problemu także można wymusić, aby na pulpicie pojawiły się skróty do niezbędnych firmowych aplikacji, a całą resztę funkcjonalności systemu Windows, włącznie z używaniem niepotrzebnych przycisków, po prostu zablokować.

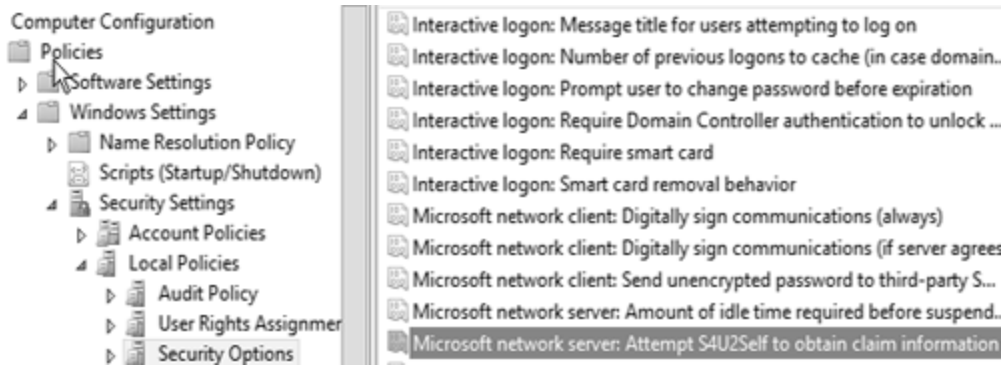
Podobnie ma się sprawa aspektów sprzętowych, jak blokowanie napędu optycznego, nośników USB itp. To tak, jakby administrator sam budował swój własny system operacyjny, idealnie spersonalizowany do potrzeb i upodobań użytkowników. Co najważniejsze, można tego dokonać w sposób łatwy i przyjemny. Istotne także jest to, że polisy można wdrożyć na potrzeby pojedynczego komputera bez konieczności korzystania z domeny. Na przykład wbudowane w system konto gościa pozostawia użytkownikom zbyt duże pole do manewru, a na komputerze domowym jest zbyt wielu gości – wystarczy więc w odpowiedni sposób zająć się polisami lokalnymi.

9.1. Wybrane nowości w GPO

Warto omówić nowości, jakie zostały wprowadzone w Windows Server 2016. Większość elementów nie uległa zmianie, jednak jest kilka różnic. Jedną z nich jest Name Resolution Policy, gdzie pojawiły się dwie dodatkowe zakładki Generic DNS Server oraz Encoding, które są związane z DNS SEC oraz rolą DirectAccess.



Pojawiła się także zasada związana z autoryzacją metodą Claim dla systemów starszych niż Windows Server 2012, o nazwie Microsoft network server: Attempt S4USelf to obtain claim information.



W gałęzi Public Key Policies pojawiły się dwa nowe kontenery. Jednym z nich jest BitLocker Drive Enryption Network Unlock Certificate, gdzie znajdują się ustawienia związane z napędami szyfrowanymi BitLockerem. Drugim jest Protection, który przechowuje ustawienia agenta odzyskiwania Data Protection Recovery Agent.

W funkcji AppLocker pojawiła się także pewna nowość. Jest nią Packaged app Rules, odpowiadający za blokowanie aplikacji napisanych dla interfejsu Metro, które między innymi można nabyć za pośrednictwem Microsoft AppStore.

Bardzo duże zmiany zaszły w Administrative Templates, co ma związek z nowym interfejsem i możliwościami systemu Windows Server 2016.

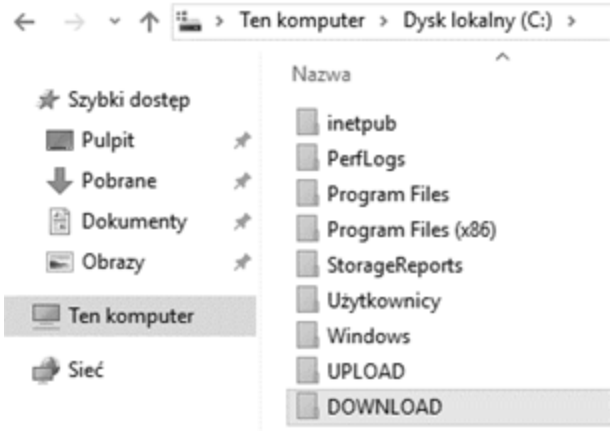
10. Uprawnienia Sieciowe i na systemie plików

Jedną z największych zalet systemu plików NTFS jest możliwość szczegółowego zarządzania dostępem do zasobów. Dzięki grupom wcześniej utworzonym w usłudze Active Directory, można swobodnie zarządzać tym, która z nich, jakie będzie miała uprawnienia. Nie mówiąc tu tylko o ustawieniach dostępu do plików, ale także do urządzeń, np. drukarek. Można tylko określonym osobom pozwolić z niej korzystać, a nawet ustawić priorytety wydruku. Na przykład, jeśli kierownik będzie miał wyższy priorytet, to drukowanie wywołane przez pracowników zostanie wstrzymane po to, aby dokumenty kierownika mogły zostać wcześniej wydrukowane. Kiedy to się stanie, wznowione zostaną wydruki o niższym priorytecie. W tym dziale

przedstawione także zostanie nadawanie uprawnień dla zasobów sieciowych. Na koniec udostępniony zasób zostanie zamapowany jako dysk twardy na komputerze klienta oraz narzucona zostanie quota na zasobie, czyli ograniczenie ilości danych, jakie będzie można w nim przechowywać.

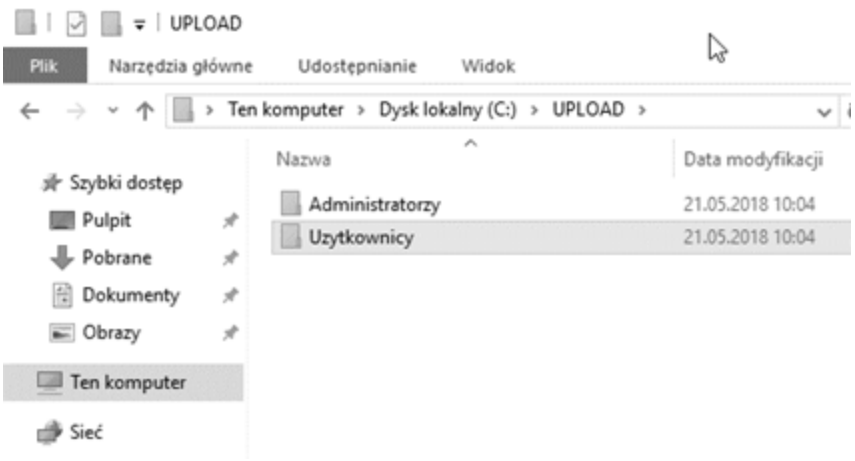
10.1. Uprawnienia sieciowe

Aby przećwiczyć nadawanie uprawnień sieciowych, warto stworzyć na dysku C katalogi UPLOAD i DOWNLOAD, które w miarę prosty sposób uda się skonfigurować.

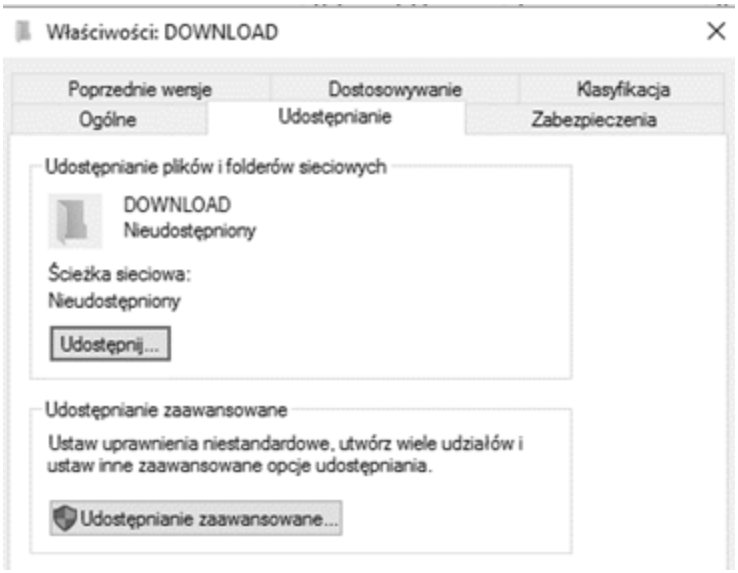


Wewnątrz obu katalogów zostaną stworzone foldery o nazwach:

- Administratorzy,
- Użytkownicy.

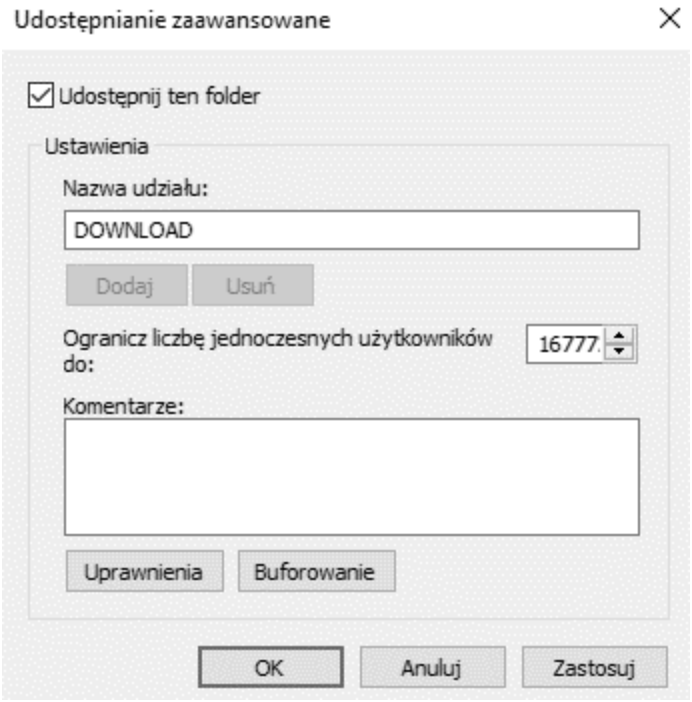


Należy kliknąć prawym przyciskiem myszy na folderze DOWNLOAD, wybrać jego Właściwości (Properties) i przejść do zakładki Udostępnianie (Sharing). Następnie należy kliknąć w Udostępnianie Zaawansowane (Advanced Sharing).

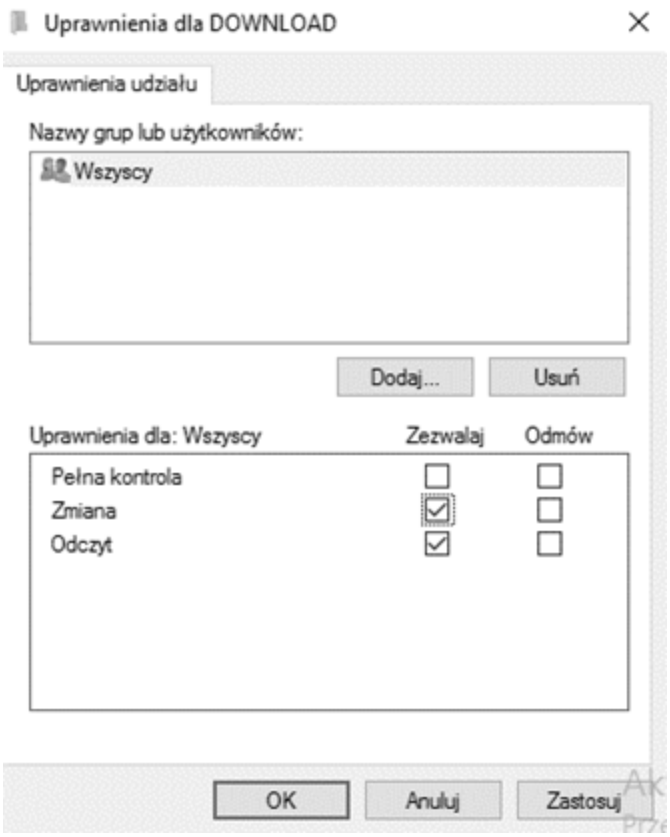


Aby folder udostępnić, konieczne jest zaznaczenie opcji Udostępnij ten folder (Share this folder). W polu Nazwa udziału (Share name) należy wpisać nazwę, pod jaką będzie on widoczny w sieci, np. DOWNLOAD. Gdyby jego nazwa została zapisana jako DOWNLOAD$, czyli na końcu nazwy dopisany by został symbol dolara, folder ten byłby

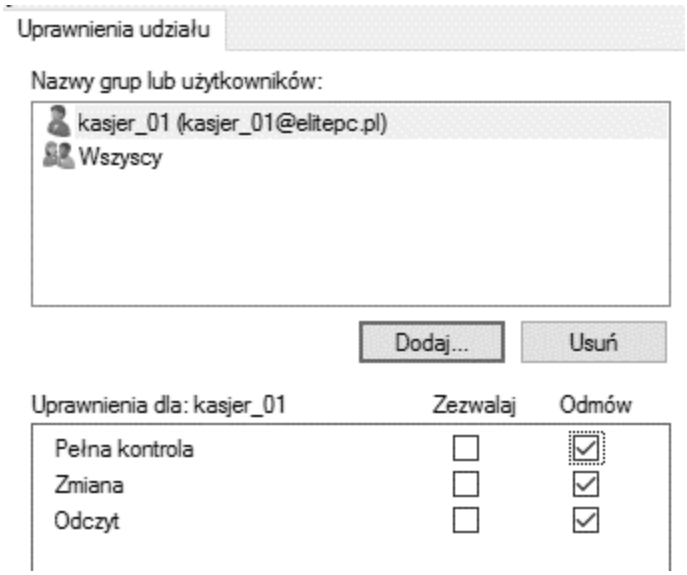
udostępniony jako ukryty. Można by było się do niego dostać np. poleceniem: \\serwer\DOWNLOAD$, natomiast nie byłby on widoczny z poziomu otoczenia sieciowego.



Klikając w przycisk Uprawnienia (Permissions), można nadawać uprawnienia dostępu sieciowego. Jest to Odczyt (Read) i Zmiana (Change) lub Pełna kontrola (Full Controll). Uprawnienia te można nadawać zarówno pojedynczym użytkownikom, jak i grupom użytkowników. Dodaje się je przyciskiem Dodaj (Add).

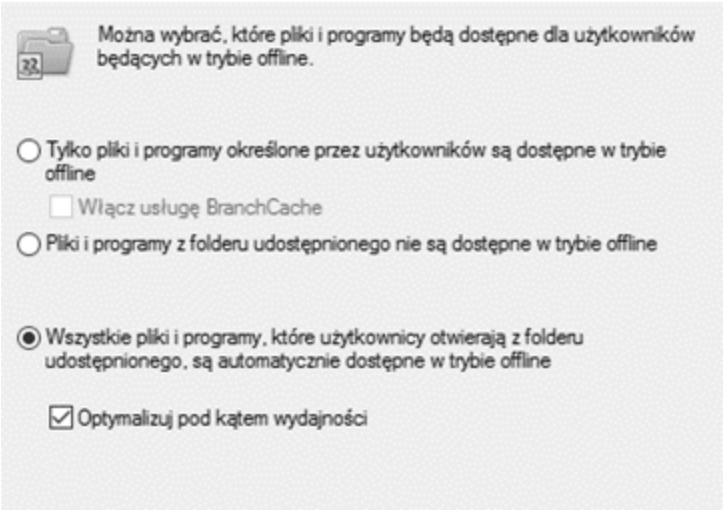


Warto zauważyć, że nadając uprawnienia, administrator ma dwie opcje: Zezwól (Allow) oraz Odmów (Deny). Ta druga jest silniejsza i służy do tworzenia wykluczeń. Dla przykładu: grupie Wszyscy (Everyone) dano możliwość Odczytu i Zmiany, a pojedynczy użytkownik, np. kasjer_01, ma nie mieć dostępu. W tym celu kasjerowi_01, zamiast w sekcji Allow nadać odpowiednie uprawnienia, zabiera się je w sekcji Deny. Mimo że należy on do grupy Wszyscy, i tak nie będzie miał dostępu do zasobów. Podobnie sprawa wygląda w przypadku nadawania innych uprawnień w systemie Windows Server 2016.



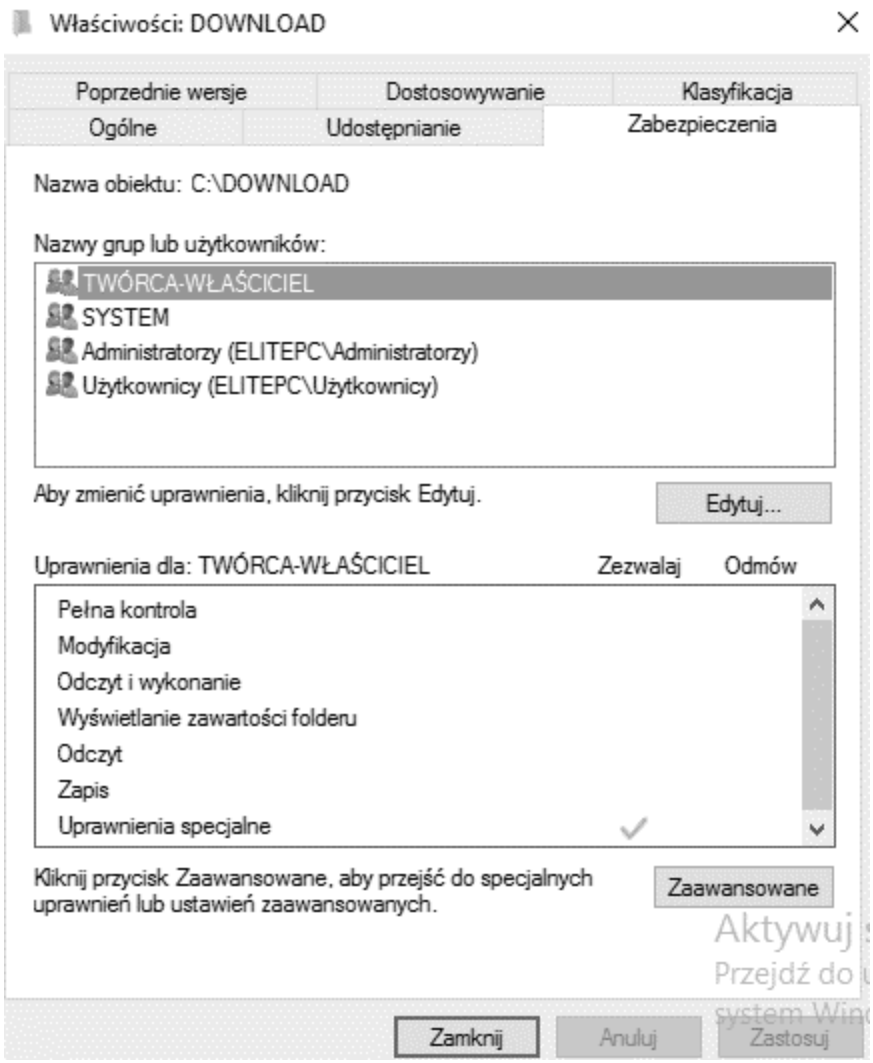
10.1.1. Dodatkowe ustawienia udostępnianych plików

Po powrocie do okna udostępniania zasobów warto kliknąć w Buforowanie (Casching). Uruchomienie tej opcji i zoptymalizowanie jej wydajności spowoduje, że użytkownik zachowa dostęp do swoich plików, nawet gdy nie będzie podłączony przez sieć do serwera. Natomiast w momencie podpięcia dane zostaną zsynchronizowane.

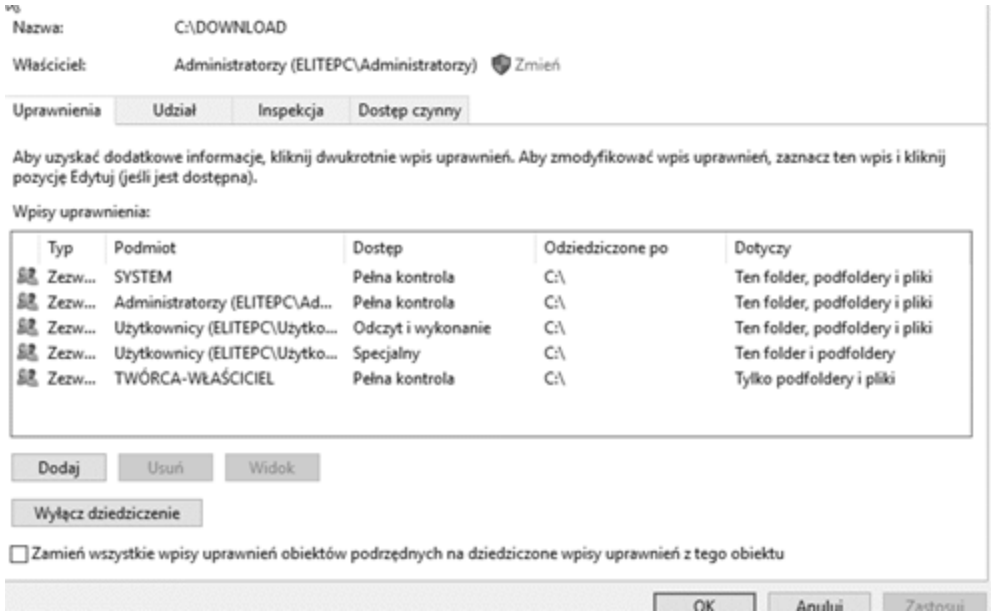


10.2. Uprawnienia NTFS

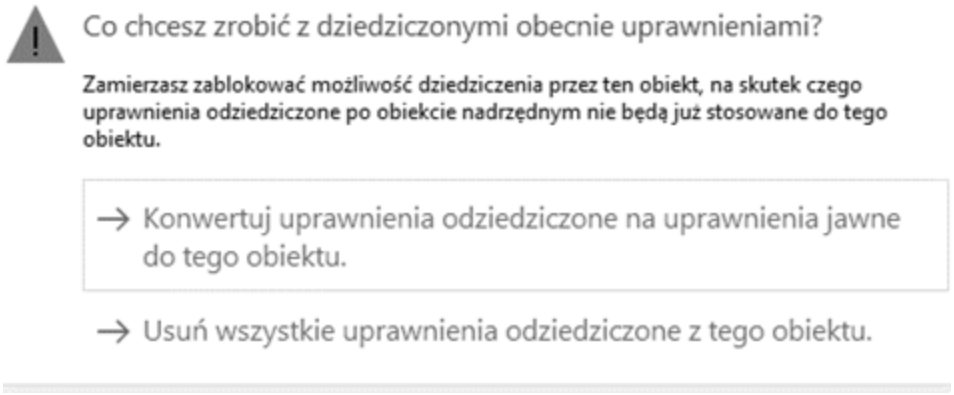
Uprawnienia na systemie plików NTFS są znacznie bezpieczniejsze i bardziej zaawansowane. W celu ich edycji należy, we właściwościach pliku bądź folderu, kliknąć w zakładkę Zabezpieczenia (Security)..



Aby można było swobodnie edytować uprawnienia NTFS, należy wyłączyć dziedziczenie z katalogu nadrzędnego. Domyślnie w systemie Windows nowo utworzony folder przejmuje uprawnienia z folderu nadrzędnego, w przypadku książkowym bezpośrednio z Dysku C. Należy wejść we właściwości folderu Administratorzy, a następnie w zakładkę Zabezpieczenia (Security) i kliknąć w przycisk Zaawansowane (Advanced), a tam wybrać opcję Wyłącz dziedziczenie (Disable inheritance) po to, aby móc swobodnie edytować uprawnienia.

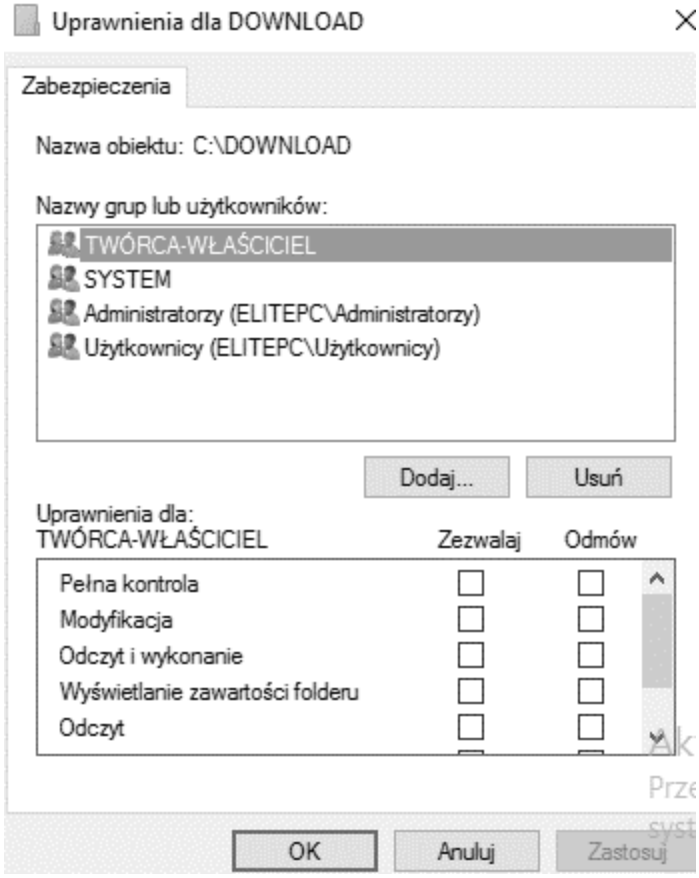


W komunikacie, który się pojawi, należy kliknąć Przekształć odziedziczone uprawnienia do jawnych uprawnień do tego obiektu (Convert inherited permissions into explicit permissions on this object). Spowoduje to przekopiowanie uprawnień tak, aby te już istniejące zostały zachowane.



Teraz, po powrocie do zakładki Zabezpieczenia (Security) i przyciśnięciu guzika Edytuj (Edit), istnieje możliwość edycji uprawnień NTFS. Jest ich więcej, są to Zapis (Write), Odczyt (Read), Listowanie zawartości folderu (List folder contents), Odczyt i Wykonanie (Read & Execute), Modyfikacja (Modify)

oraz Pełna kontrola (Full Control), która między innymi pozwala na edycję uprawnień.



Warto zwrócić uwagę, że nie ma potrzeby ograniczania się do grup, gdyż uprawnienia można także spersonalizować dla pojedynczego użytkownika. Czasami np. dla kierownika działu jest to pożądane. Często zdarzają się sytuacje, gdy w przypadku plików lub folderów tylko jedna osoba ma mieć możliwość ich edycji, a jej współpracownicy jedynie mogą ten plik odczytywać. W taki sposób można więc łatwo nadać uprawnienia pojedynczemu użytkownikowi do edytowania.

Twórca-właściciel ma nadane specjalne uprawnienia, których też lepiej nie edytować bez doświadczenia w tej kwestii. Należy też pamiętać, że wcześniej modyfikowane

były uprawnienia dostępu przez sieć, a teraz modyfikowany jest dostęp do plików na dysku, a nie zasobów udostępnionych. Trzeba także uważać i wiedzieć, co się robi. Dla przykładu: Użytkownikom odmówiona zostanie możliwość odczytu, a Administratorowi będzie to dozwolone. Pojawia się pytanie, czy Administrator będzie mógł odczytać zasoby, bo przecież on też jest Użytkownikiem. W ramach książki zostaną zmodyfikowani Użytkownicy tak, aby nie mieli żadnych uprawnień do zasobów. Resztę można zostawić bez zmian.

W przypadku katalogu Download, w celach testowych zwykli użytkownicy nie dostaną żadnych praw.

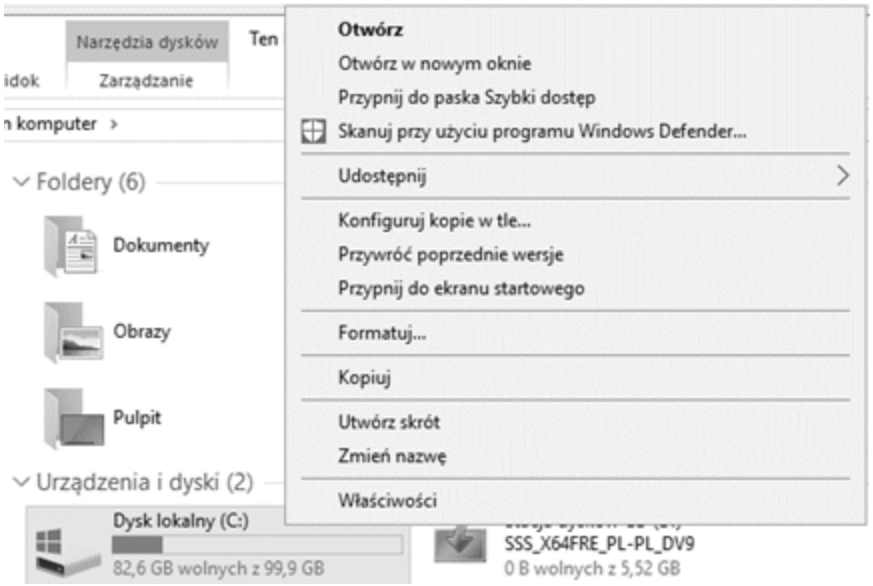
W przypadku katalogu Upload, użytkownicy dostaną jedynie możliwość Zapisu i wykonania. Modyfikować nic nie muszą, a Pełna Kontrola by im pozwoliła zmieniać uprawnienia folderów i plików. Nie tylko byłoby to niebezpieczne ze względu na brak umiejętności z ich strony, ale Administrator powinien być jedyną osobą z takimi możliwościami. Na stronach technet można znaleźć dokładny opis tego, za co dane uprawnienie odpowiada. Warto się temu zagadnieniu przyjrzeć, gdyż pozwala to na wygodne zarządzanie dostępem do plików dowolną drogą. Nie jest ważne, czy przez sieć lokalną, FTP czy stronę www, te ustawienia zawsze są brane pod uwagę.

UWAGA!!!

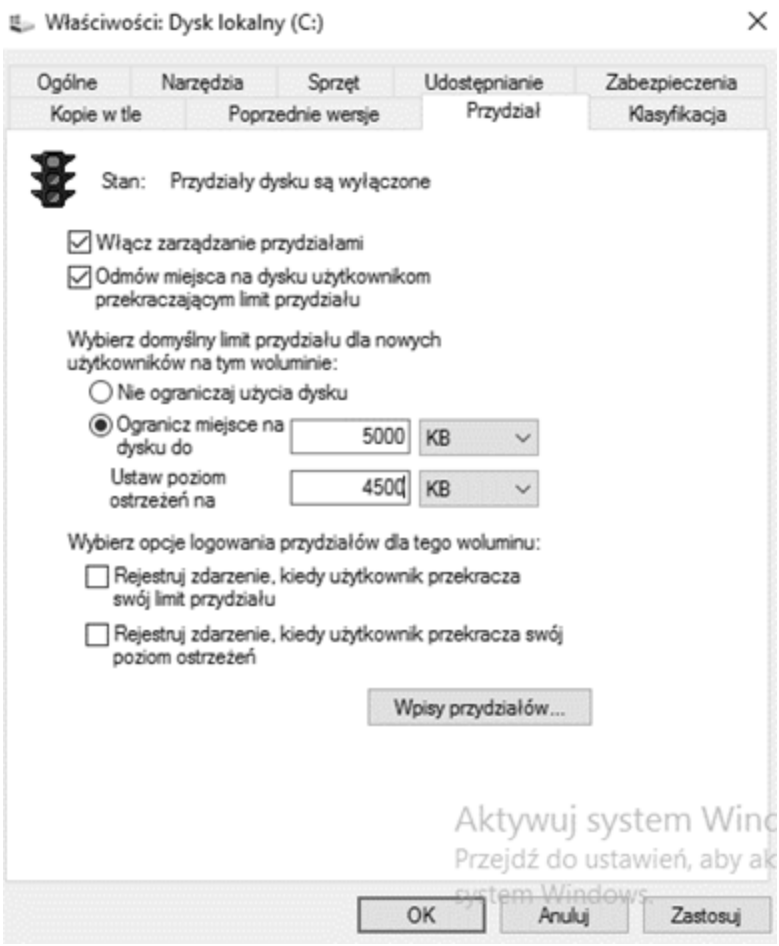
Gdy folder kopiowany jest do innej lokalizacji, nałożone na niego uprawienia są tracone i dziedziczy on nowe

uprawnienia z folderu nadrzędnego. W przypadku, gdy folder jest przenoszony, uprawnienia są zachowywane.

Aby włączyć limit na wolumenie, należy kliknąć prawym przyciskiem myszy na dysku i wybrać Właściwości (Properties).



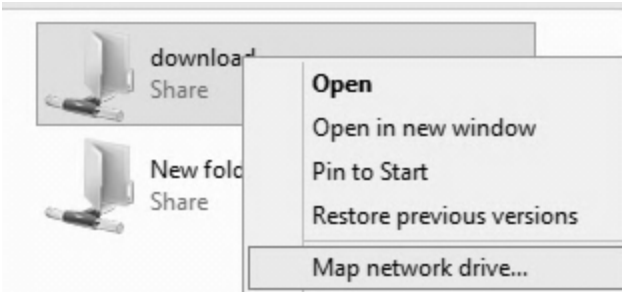
Następnie należy wybrać Przydział (Quota). Zostanie uruchomione zarządzanie przydziałami i skonfigurowane tak, jak na zrzucie z ekranu poniżej. Spowoduje to, że użytkownik nie będzie mógł na dysku C serwera przechowywać więcej niż 5000 MB danych, a gdy przekroczone zostanie 4500 MB, pojawi się komunikat z ostrzeżeniem. Co więcej, nie jest ważne, gdzie dany użytkownik ma umieszczone swoje pliki, ważna jest suma ich rozmiarów. System je odnajdzie po właściwości zasobu mówiącej o jego właścicielu. Należy kliknąć w Zastosuj (Apply) i OK.



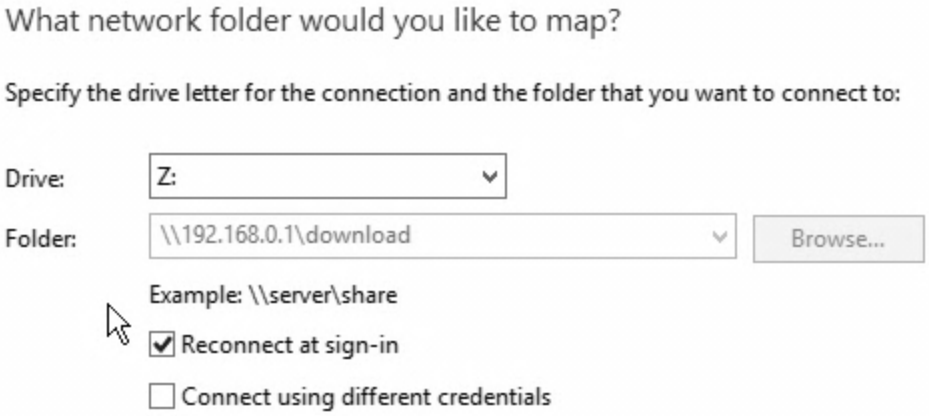
Warto wykonać kilka testów, czy nałożone wcześniej uprawnienia i Quota działają, przechodząc do komputera klienckiego i logując się na nim jako Kasjer. Konieczne jest wejście w Mój Komputer (My Computer) i w panelu z lewej strony okna wybranie z menu Sieć (Network) nazwy komputera, do którego zasobów można się dostać. Pojawi się lista udostępnionych zasobów. Przykładowo, można więc wybrać Download. Niestety, zwykły użytkownik nie ma praw dostępu do tego katalogu, co jest prawidłowe we wcześniejszej konfiguracji.

Teraz pora zapewnić łatwy dostęp do tych katalogów. Najlepiej będzie je zamapować jako dyski sieciowe.

W przypadku książkowym najprościej jest to zrobić, klikając w dany folder prawym guzikiem i wybierając opcję Mapuj dysk sieciowy (Map Network Drive).



Można wybrać literę dysku i ewentualnie wprowadzić poświadczenia innego użytkownika, aby to z jego uprawnieniami dysk był zmapowany. Na koniec należy kliknąć Zamknij (Finish).



10.3. Autoryzacja metodą CLAIM

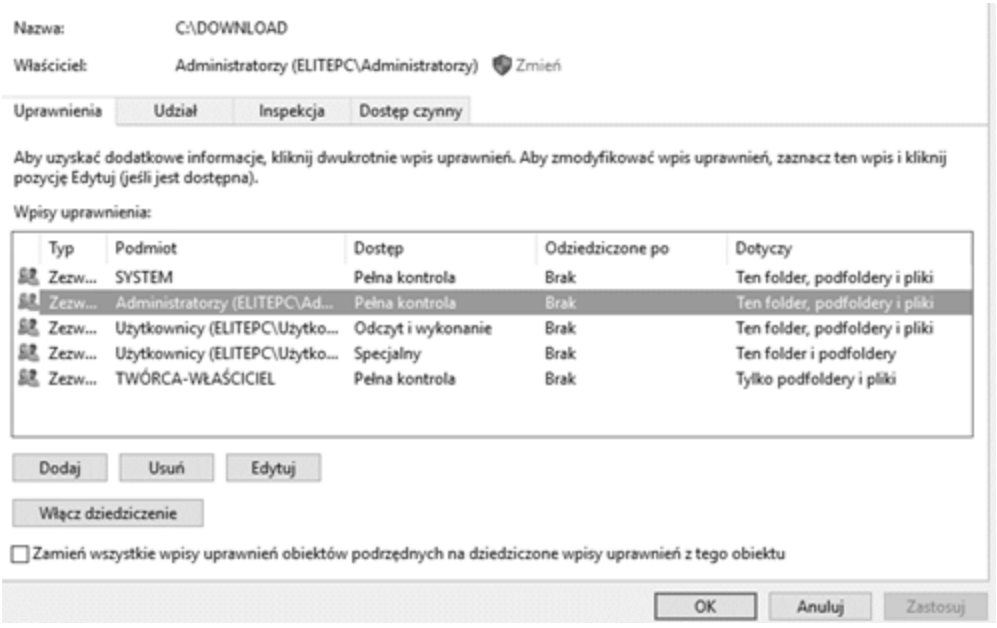
W tym rozdziale omówiony zostanie mechanizm autoryzacji metodą Claim. Sam w sobie nie jest on nowością. Wcześniej był on z powodzeniem używany w Active Directory Federation Services w Windows Server

2008 R2. To, co się zmieniło to to, iż teraz może on być używany w obrębie lasu czy też domeny. Ten mechanizm rzuca całkowicie nowe światło na metody autoryzacji. Może on być używany np. podczas autoryzacji dostępu do danych udostępnianych przez serwer plików przy użyciu tzw. Uzgodnień (Claim) zapisanych w atrybutach konkretnego obiektu, które mogą być zdefiniowane na poziomie Active Directory.

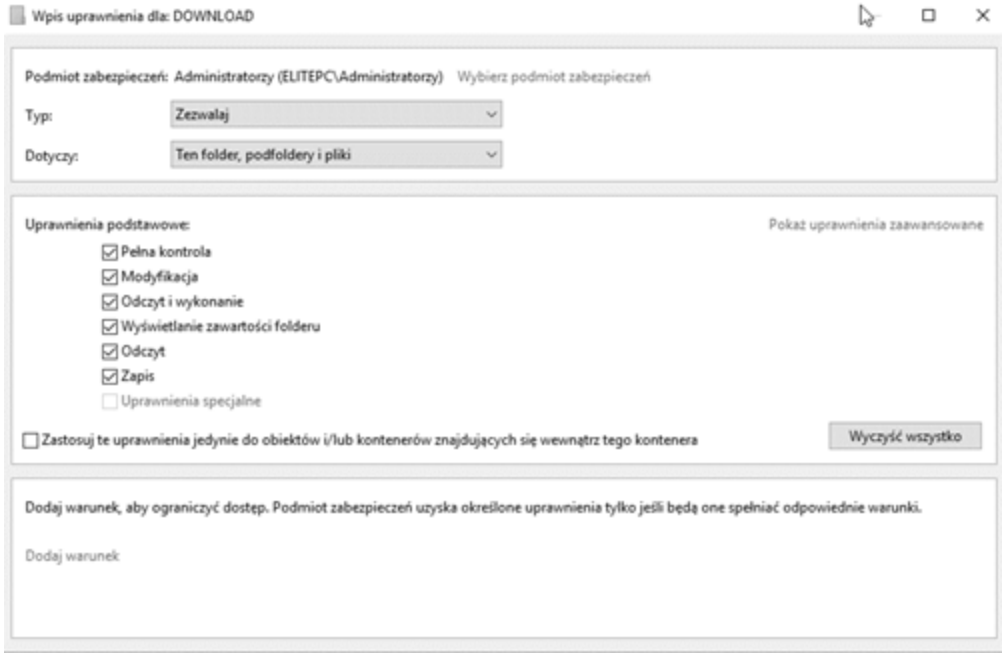
10.3.1. Nakładanie uprawnień Claim

Do tej pory uprawnienia były nadawane za pomocą tzw. List Kontroli Dostępu (Access Control List). Określane było jacy użytkownicy, grupy czy komputery mają mieć dostęp do zasobów i z jakimi uprawnianiami (Allow/Deny). Następnie te dane były przekazywane jako token w protokole Kerberos. To w systemie Windows Server 2016 się nie zmieniło.

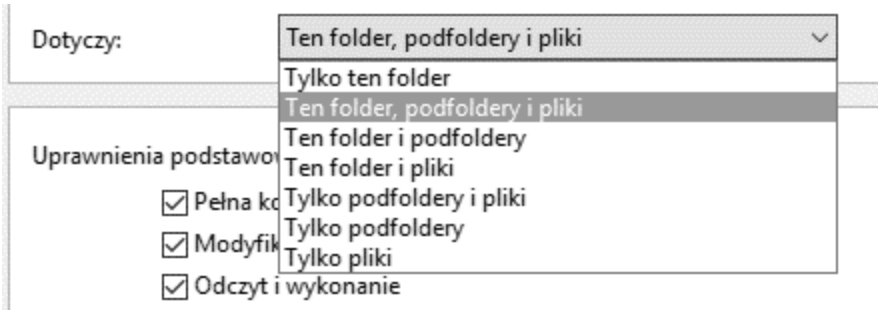
Okno zaawansowanego udostępnienia pozornie uległo jedynie zmianom kosmetycznym. Lecz to nie do końca prawda.



Zostanie wyłączone dziedziczenie. Warto zauważyć, że po dwukrotnym kliknięciu w użytkownika, czy też grupę, lub przy dodawaniu nowej pozycji do listy DALC pojawiają się nowe opcje związane z autoryzacją metodą CLAIM.



Na powyższym zrzucie ekranu widać nowe okno nadawania uprawnień do obiektu. W pierwszej kolejności należy wybrać podmiot, którym może być dowolny użytkownik lub dowolna grupa użytkowników. Po wybraniu podmiotu należy zdefiniować, czy reguła będzie pozwalała wykonywać jakąś czynność, czy też nie (Allow/Deny), a także zdefiniować, jaki jest zasięg reguły.



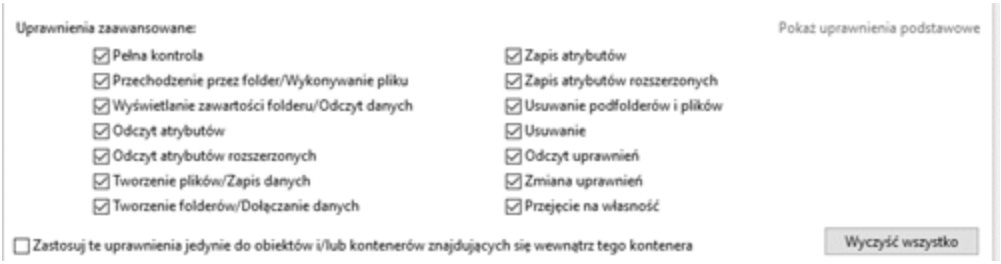
Może się ona tyczyć kolejno:

- Tylko tego folderu,
- Tego folderu, pod folderów oraz plików,
- Tego folderu i podfolderów,
- Tego folderu i Plików,
- Tylko podfolderów i plików,
- Tylko podfolderów,
- Tylko plików.

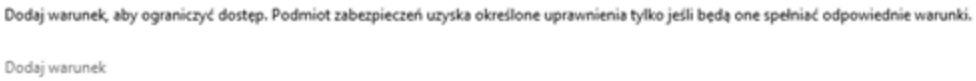
Następnie w sekcji Uprawnienia (Permissions) należy zdefiniować odpowiednie uprawnienia. Do wyboru jest Pełna Kontrola (Full Control), która między innymi pozwala zarządzać uprawnieniami, możliwość Modyfikowania (Modify) zawartości folderu, Odczytu i Wykonania (Read & Execute), Przeglądania zawartości folderu (List folderdcontents), Odczytu (Read), a także Zapisu (Write).

Jeżeli są niewystarczające, można także skorzystać z uprawnień zaawansowanych (Show advanced permissions). Są one dużo bardziej precyzyjne. Zdefiniować można, podobnie jak wcześniej, pełną kontrolę (Full control) lub jedynie wybrać któreś z pozostałych możliwości, którymi są kolejno: przechodzenie pomiędzy folderami i wykonywania plików (Traverse folder/ execute folder), listowanie zawartości folderów i odczyt danych (List folder

/read data), odczyt atrybutów (Read attributes), odczyt atrybutów rozszerzonych (Read extended attributes), tworzenie plików i zapis danych (Create files/ write data), tworzenie folderów i dołączanie danych (Create folders /append data), zapisywanie atrybutów (Write attributes), zapisywanie rozszerzonych atrybutów (Write extended attributes), kasowanie podfolderów i plików (Delete subfolders and files), kasowanie (Delete), możliwość odczytu (Read permissions), możliwość zmiany (Change permissions), możliwość przejmowania na własność (Take ownership).

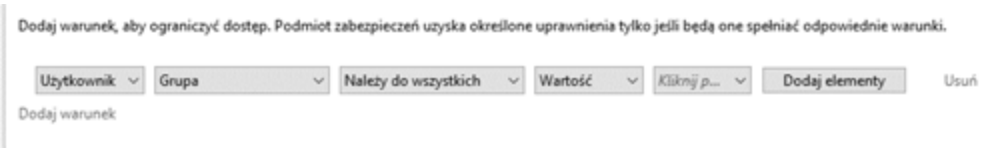


Ostania trzecia już sekcja okna dotyczy tworzenia reguły autoryzacyjnej. To właśnie one stanowią metodę autoryzacji CLAIM. Standardowo żadna reguła nie jest zdefiniowana i brane są pod uwagą uprawnienia nadane w zwykły sposób. Aby taką regułę dodać, należy kliknąć Dodaj Warunek (Add Condition).

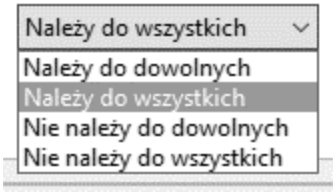


Spowoduje to pojawianie się dodatkowej listy, w której istnieje możliwość zdefiniowania warunków dostępowych. W pierwszym polu określa się, czy reguła będzie dotyczyła użytkownika (User) czy urządzenia, czyli konta komputera

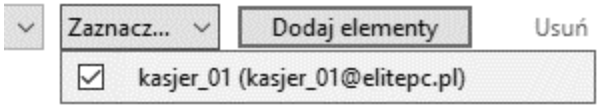
(Device). W drugim polu należy określić, czy reguła dotyczyć będzie jakiejś grupy.



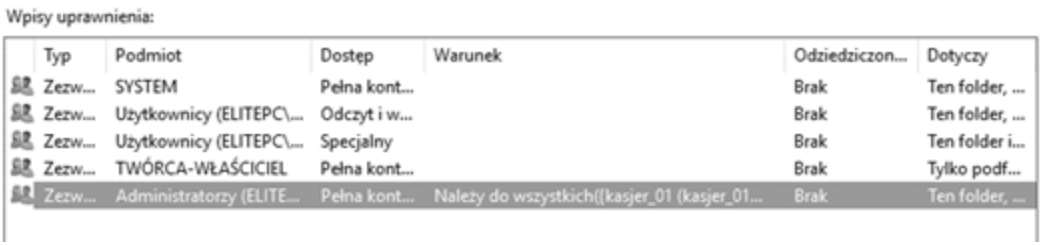
W trzecim określa się, czy reguła będzie obowiązywała użytkowników należących do jednej z grup wyznaczonych w polu piątym, czy też użytkowników należących do każdej z grup lub niebędących członkami ani jednej z tych grup lub niebędących członkami wszystkich tych grup.



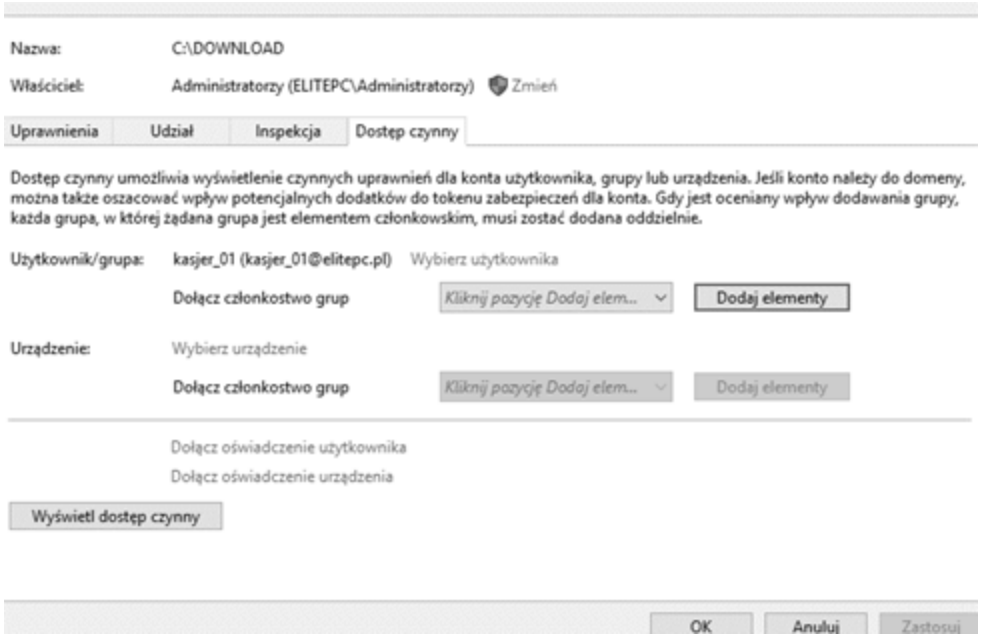
Przyciskiem Dodaj obiekty (Add items) można zdefiniować, jakich grup będzie dotyczyła reguła.



Tak utworzona reguła pojawi się na liście.

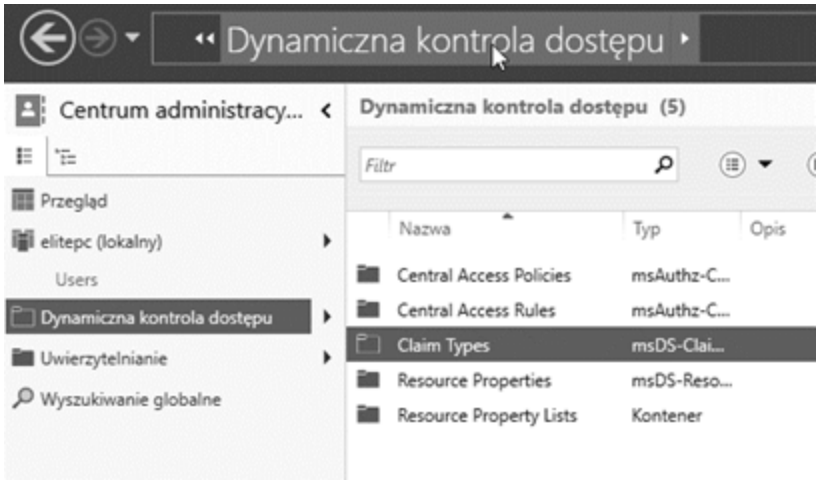


W zakładce Efektywne Uprawnienia (Effective Access) istnieje możliwość podejrzenia, jaki użytkownik ma uprawnienia do konkretnego folderu.

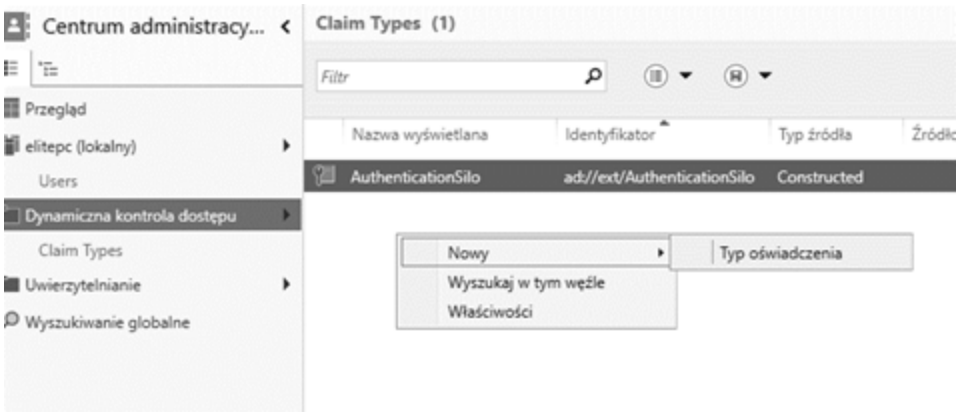


10.3.2. Definiowanie Claim Types

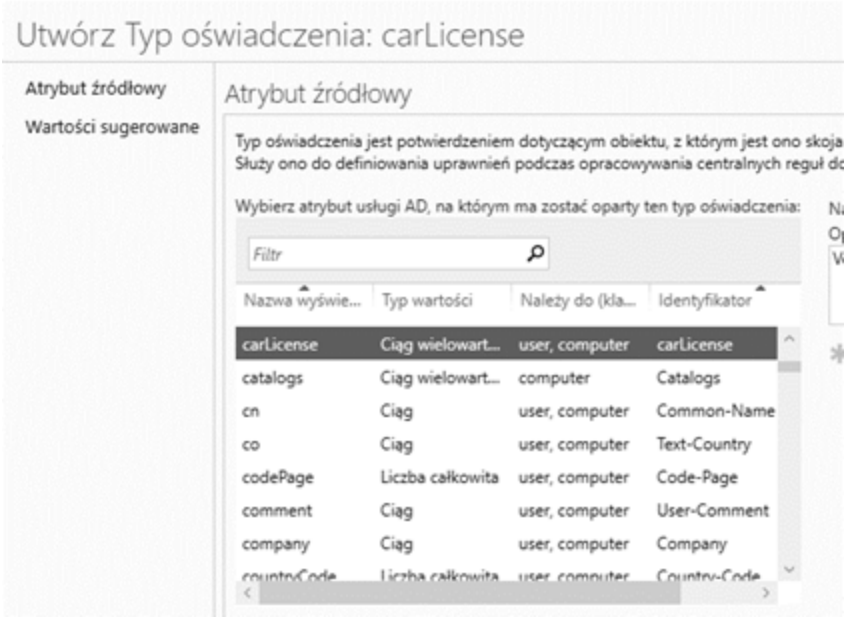
Innym sposobem definiowania uzgodnień Claim jest użycie konsoli Centrum Administracyjnego Active Directory (Active Directory Administrative Center). Należy w nim rozwinąć Dynamiczną kontrolę dostępu (DYNAMIC ACCESS CONTROL) i wybrać z listy Typy uzgodnień (Claim Types).



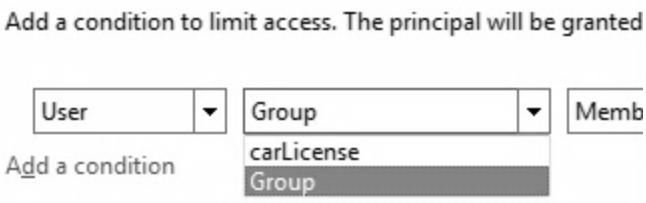
Następnie w menu po prawej stronie należy wybrać Nowy > Typ uzgodnień (New > Claim Type).



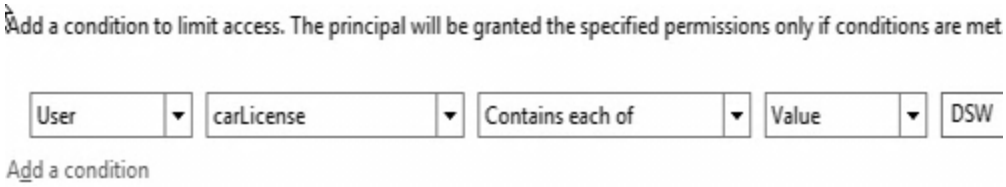
Zamiast bazować na grupach komputerów i użytkowników, można stworzyć uzgodnienie, które będzie brało pod uwagę konkretne atrybuty obiektów znajdujących się w bazie Active Directory. Dla przykładu zostanie wybrana opcja Prawo jazdy (CarLicense). Należy kliknąć OK.



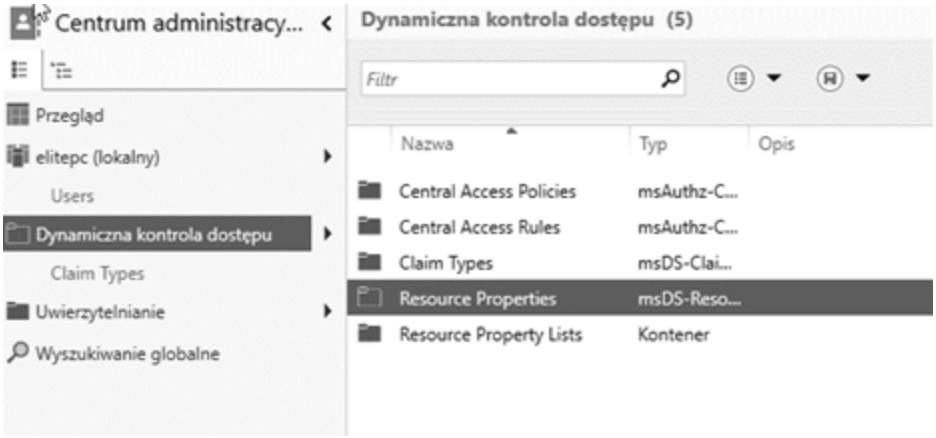
Wracając do właściwości udostępnionego folderu i próbując raz jeszcze dodać regułę CLAIM, do wyboru poza grupą pojawił się stworzony przed chwilą carLicense.



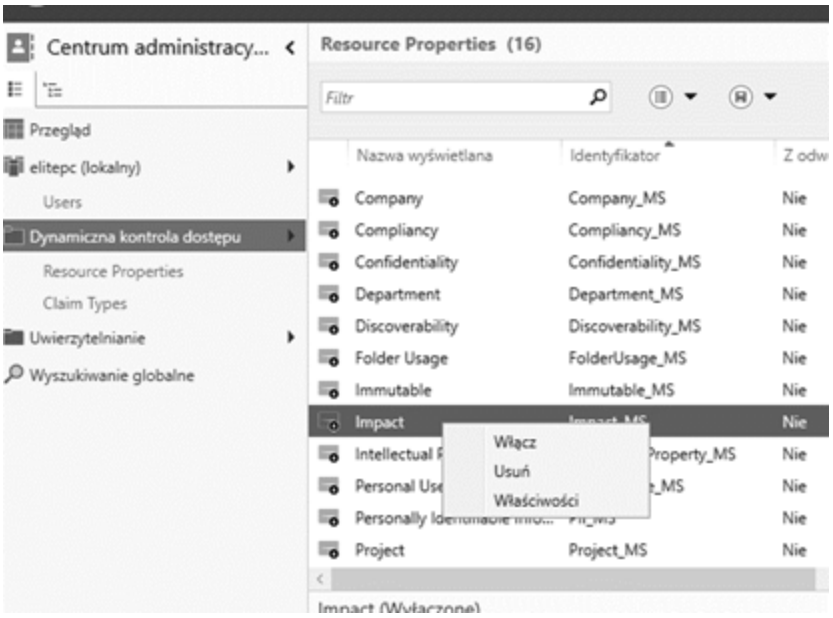
Po jego wybraniu definicja reszty reguły ulega dynamicznej zmianie w zależności od wybranych atrybutów w Centrum Administracyjnym.



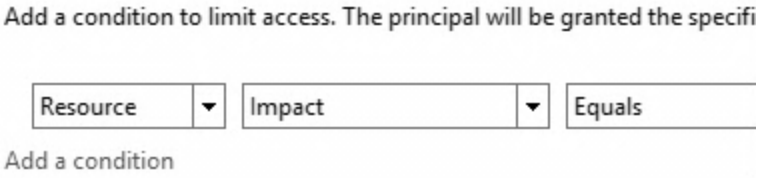
Co więcej, w podobny sposób można zdefiniować konkretne typy zasobów.



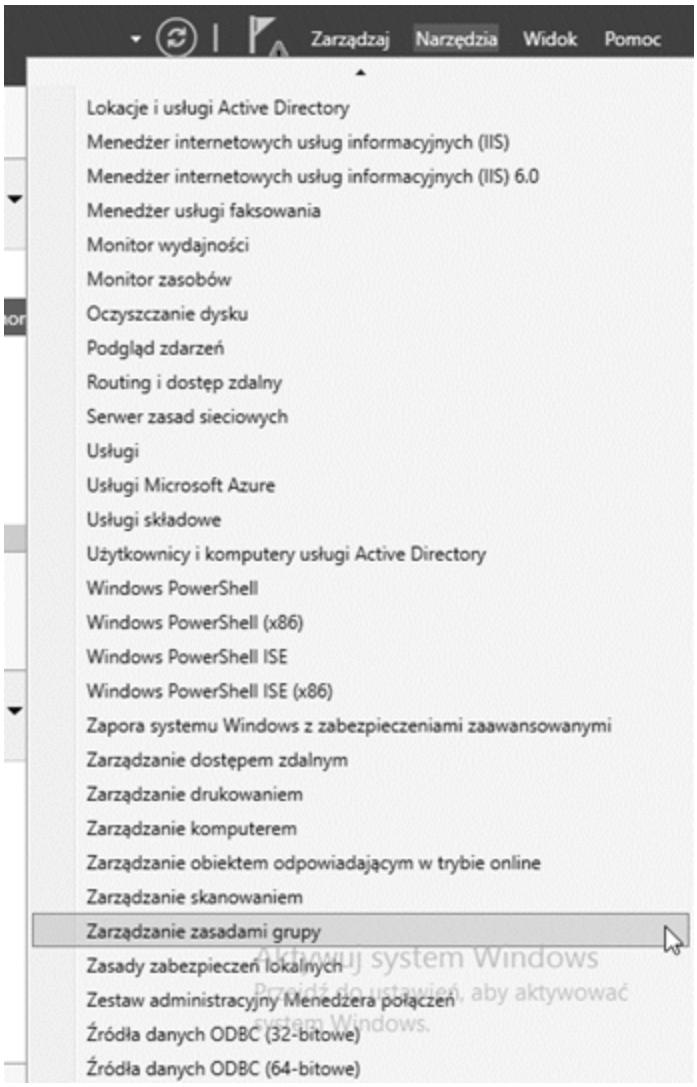
Na konkretnym typie zasobu wystarczy kliknąć prawym guzikiem i wybrać opcję Włącz (Enable).



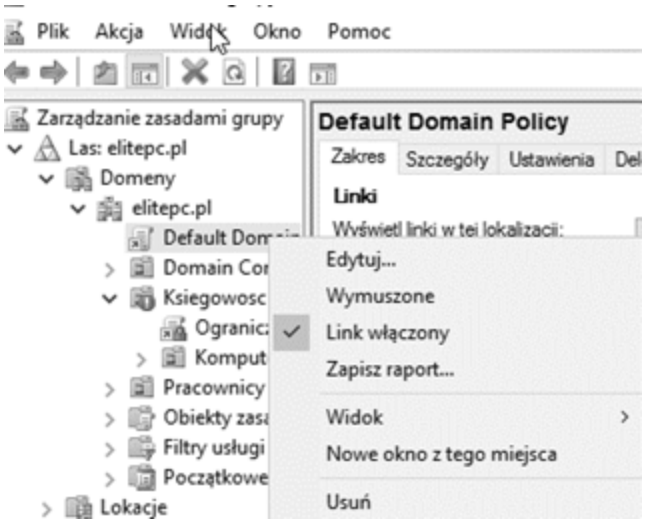
Zasób pojawi się do wyboru we właściwościach pliku/folderu.



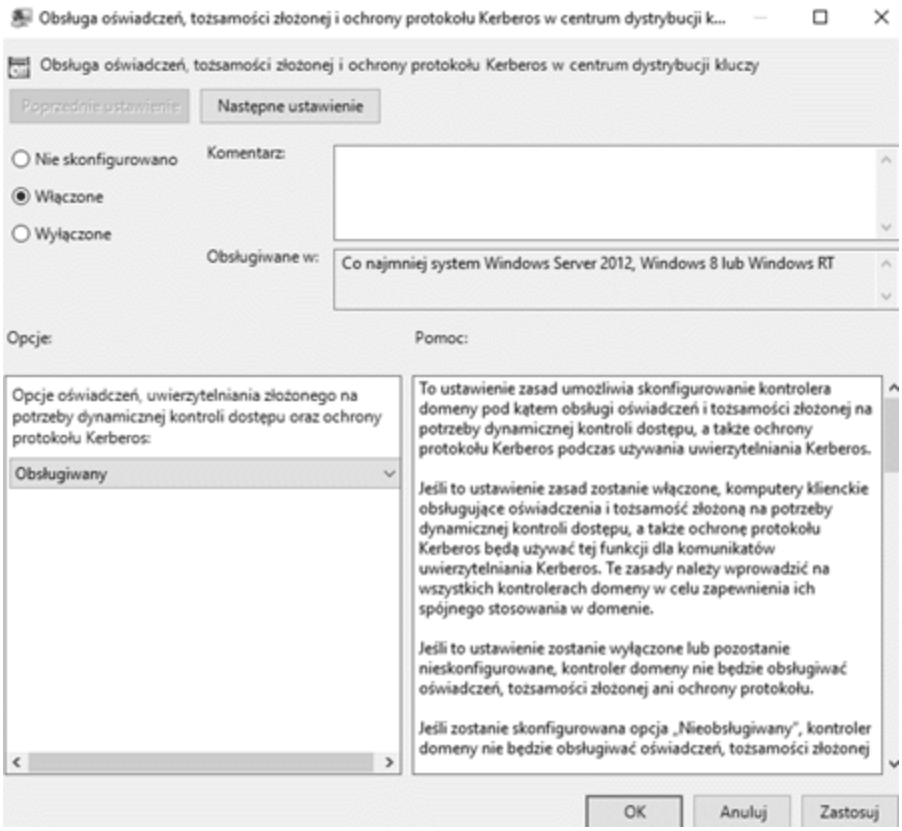
Aby dodatkowo zdefiniowane uzgodnienia Claim działały, należy jeszcze uruchomić odpowiednią polisę. Z poziomu Menadżera Serwera (Server Manager) należy wybrać Narzędzia (Tools), a następnie Group Policy Management.



Potem należy edytować Domyślną polisę domeny (Default Domain Policy) i przejść kolejno: Computer Configuration > Policies > Administrative Templates > System > KDC.



Teraz trzeba włączyć opcję KDC support for claims, compound authentication and Kerberos armoring. W testowym środowisku są kontrolery domeny pracujące na Windows Server 2016 – zatem wybrano ustawienie Support w Claims, compound authetication for Dynamic Access Control and Kerberos armoring. Modyfikacje tego ustawienia pokazuje poniższy zrzut z ekranu.



10.4. Uprawnienia na systemie plików ReFS

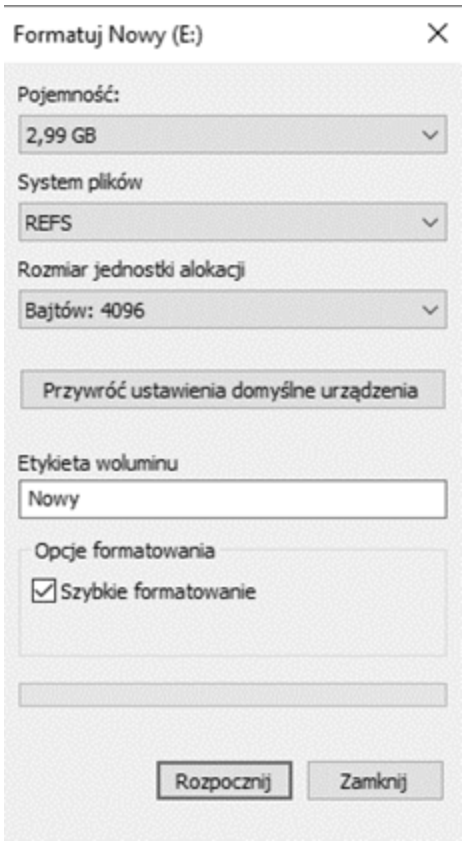
System Windows Server 2016 wprowadza jeszcze jedną znaczącą nowość. Mianowicie nowy system plików. Choć NTFS sprawdza się dobrze, to ma on już swoje lata, bo zadebiutował w 1993 roku. Nowy system plików trudno nazwać rewolucją w zarządzaniu danymi, jest to raczej ewolucja i spokojnie można by było go oznaczyć jako kolejną wersję NTFS'a. Właściwie to jest to bardziej dopracowany i zoptymalizowany NTFS.

Nazwa ReFS to skrót od Resilient File System, czyli odporny system plików. Jest on odporniejszy na

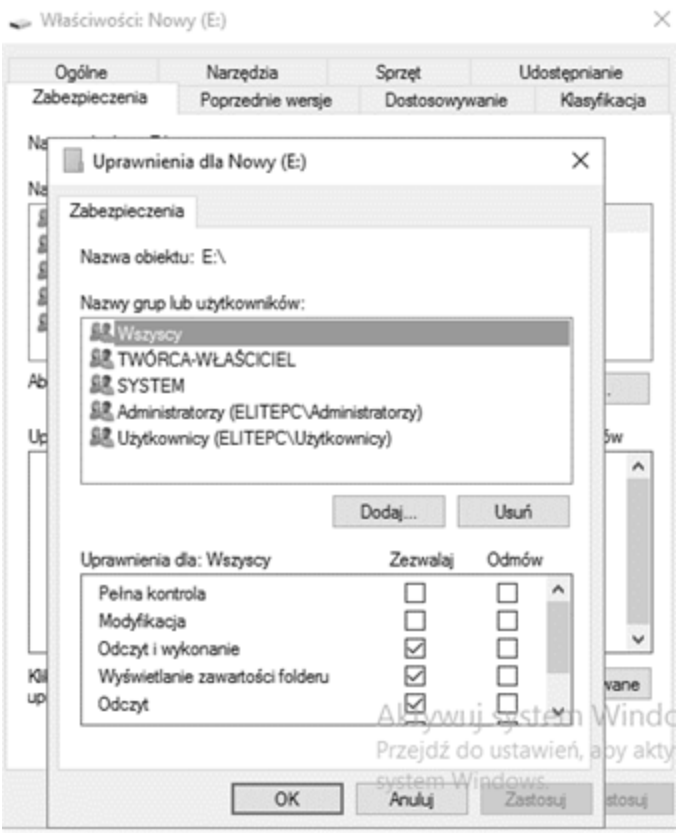
uszkodzenia zarówno logiczne, jak i fizyczne nośników.

Oferuje własne mechanizmy ochronne, takie jak sumy kontrolne, rozproszony log transakcyjny, przeprowadzanie zapisu w separacji od oryginalnego pliku itd., ale też współpracuje z mechanizmem Storage Spaces w Windows Server 2016. Dane i metadane są przechowywane w formie bardzo podobnej do relacyjnych baz danych. Dodatkowe zabezpieczenie stanowi kopiowanie przy zapisie, a także możliwość skasowania uszkodzonego pliku bez potrzeby odłączania dysku. Limity rozmiarów zostają zwiększone do 64 potęgi liczby 2. Z systemu NTFS pozostanie większość elementów interfejsu dostępu do danych, a co za tym idzie, zmianom uległ głównie wewnętrzny mechanizm działania, a nie sposób zarządzania z punktu widzenia administratora systemu. Choć interfejs jest wręcz identyczny jak w przypadku NTFS, to zniknęły niektóre funkcje, np. zabrakło szyfrowania EFS i kompresji plików bądź folderów. Na tę chwilę nie ma możliwości zainstalowania systemu operacyjnego na partycji ReFS. Microsoft prawdopodobnie chce system najpierw dokładnie przetestować, dlatego wdraża go fazami. Najpierw nowy system plików zagości w Windows Server 2016, potem w systemach klienckich, a na samym końcu dostanie możliwość pracy jako system plików na dysku rozruchowym.

W ramach ćwiczeń można jednak sformatować wybraną partycję do nowego systemu plików.



Gdy proces dobiegnie końca, można wejść we właściwości jakiegoś folderu utworzonego na tym dysku, aby zobaczyć, iż zarządzanie uprawnieniami na systemie plików ReFS nie różni się niczym od tego znanego z NTFS.

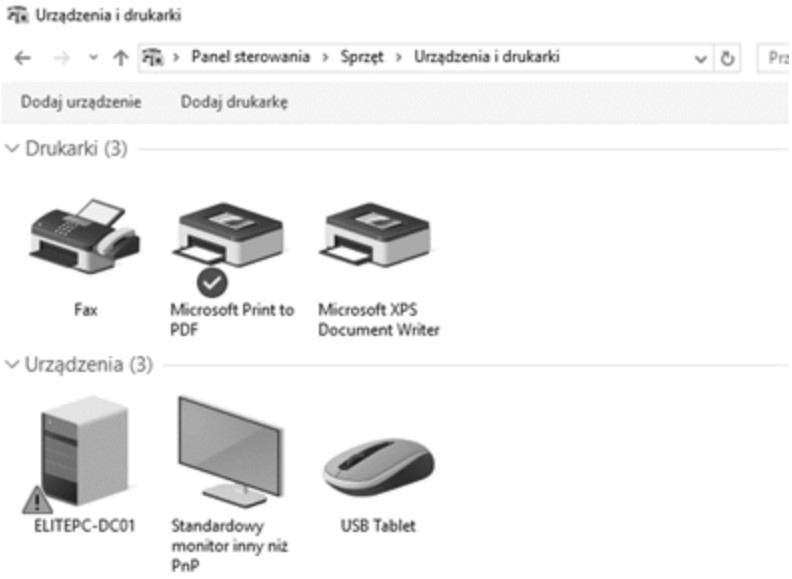


10.5. Zarządzanie drukarkami

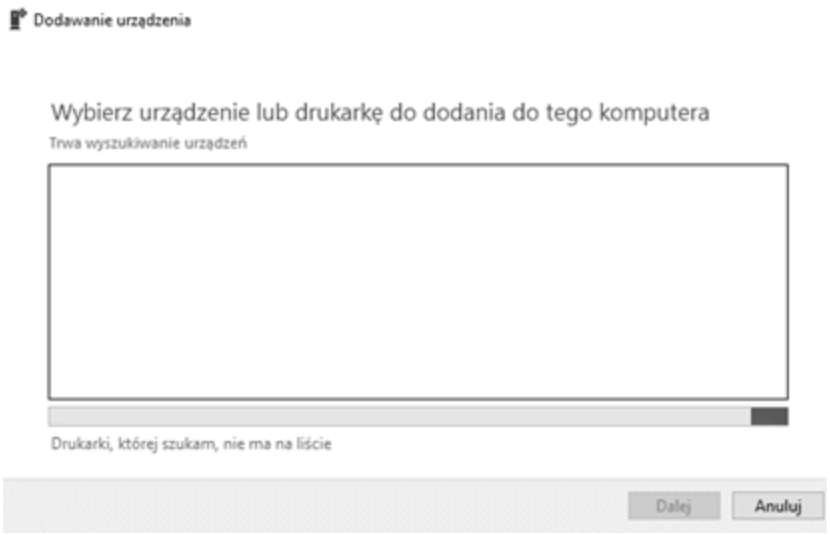
Podobnie jak w przypadku plików, uprawnienia można również nakładać na urządzenia pracujące bądź udostępnione w sieci. Dzięki funkcjom dostępnym w Windows Server 2016 administrator może efektywnie zarządzać dostępem do urządzeń i drukarek, wydajnie je udostępniać, zapewniając bezpieczeństwo działania i hermetyczność przekazywanych danych. Co więcej, może on także nadawać różne priorytety dla mniej i bardziej uprzywilejowanych pracowników przedsiębiorstwa.

10.5.1. Instalowanie drukarek

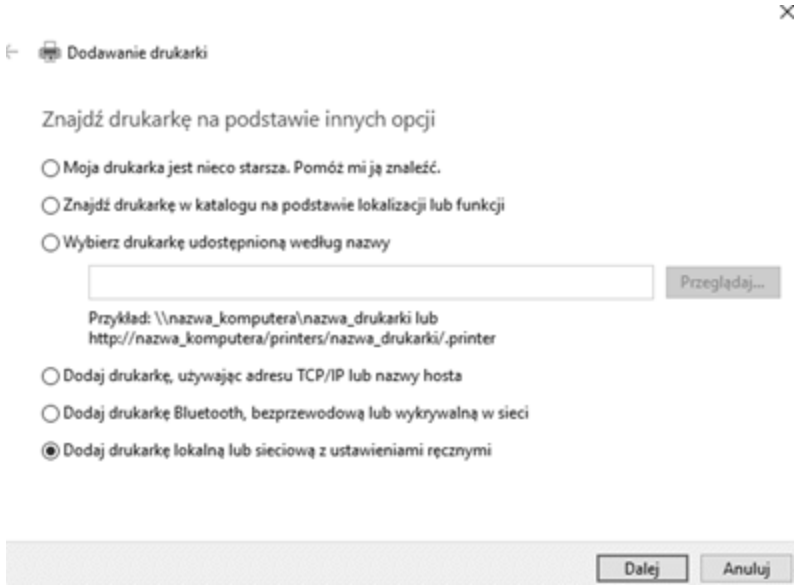
W pierwszej kolejności należy otworzyć Panel sterownia (Control panel), wybrać Sprzęt (Hardware), a następnie Urządzenia i drukarki (Devices and Printers).



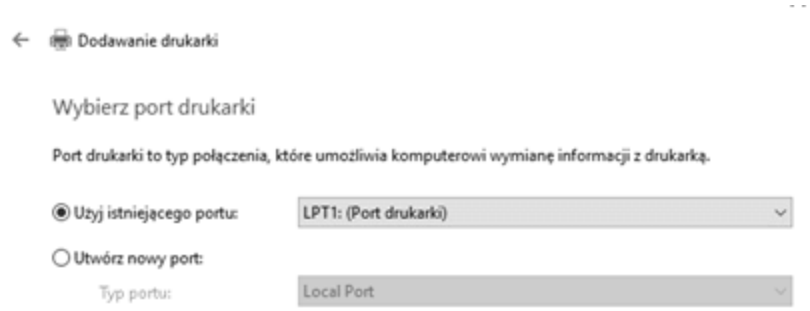
Aby zainstalować drukarkę, należy kliknąć przycisk Dodaj Drukarkę (Add a printer). W pierwszej karcie kreatora system przeskanuje urządzenia w poszukiwaniu drukarki, jeżeli takowej nie znalazł, bądź istnieje potrzeba instalacji drukarki, która fizycznie nie jest podpięta do komputera, należy kliknąć opcję Drukarka, którą pragnę zainstalować nie znajduje się na liście (The printer that I want isn’t listed).



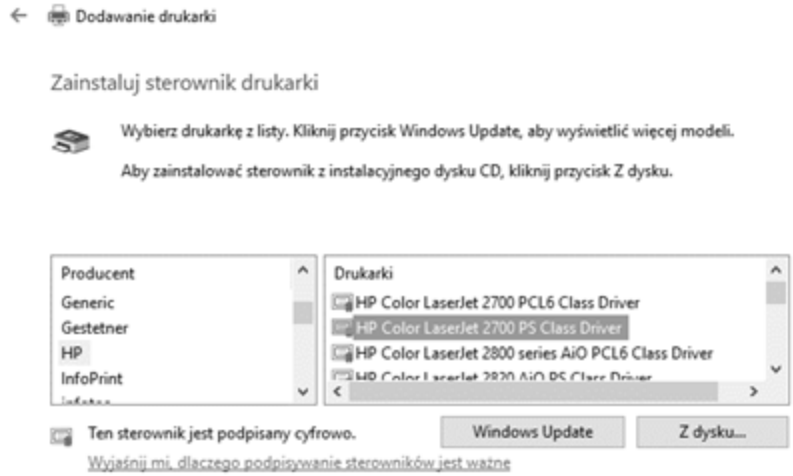
Na kolejnej karcie kreatora, w ramach ćwiczenia, w środowisku wirtualnym powinno się wybrać opcję Dodaj drukarkę lokalną lub sieciową z ustawieniami ręcznymi (Add a local printer or network printer with manual Settings).



Na kolejnej karcie warto zostawić ustawienia domyślne.



Z listy sterowników przykładowo można wybrać drukarkę firmy HP, Color LaserJet 2700PS Class Driver.



Na kolejnej karcie należy nadać drukarce nazwę, np. Drukarka Szefa. Następnie można zainstalować raz jeszcze tą samą drukarkę, nadając jej nazwę, np. Drukarka Pracownika.

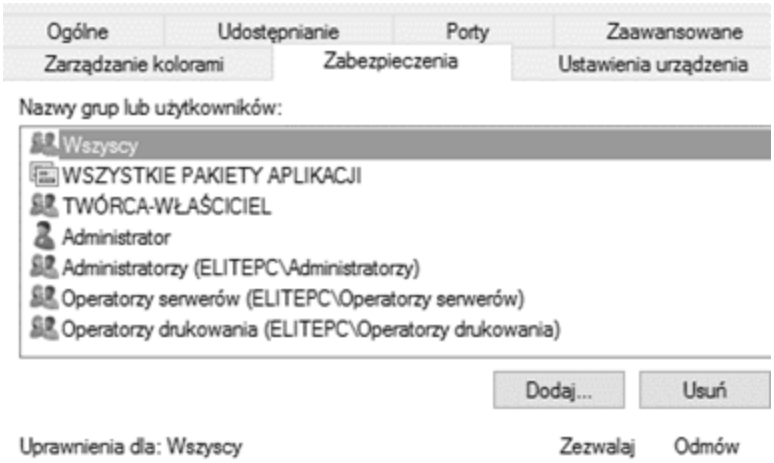
10.5.2. Zarządzanie dostępem do drukarek sieciowych

Należy wejść we Właściwości drukarki (Printer Properties).

W zakładce Udostępnianie (Sharing) można udostępnić drukarkę w sieci (analogicznie jak w przypadku plików), a także dodać sterowniki. Na przykładurządzenia często wymagają innych sterowników w zależności od wersji systemu Windows. Jeśli wszystkie zostaną tutaj dodane, to instalacja na klienckich komputerach przebiegnie bez potrzeby dostarczania CD producenta.

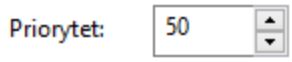
Zakładka Zaawansowane (Advanced) pozwala na ograniczenie godzin w jakich można korzystać z urządzenia za pomocą opcji Dostępna od (Available from) (podobne ograniczenia można też nakładać na użytkowników). Jest także możliwość ustawiania priorytetów. Im wyższy priorytet, tym urządzenie ważniejsze. O zastosowaniu było wspomniane wcześniej, za chwilę pokazane będzie, jak wdrożyć system kolejkowania zleceń.

Zakładka Zabezpieczenia (Security) odpowiada za dostęp do zasobów drukarki. Działa to podobnie jak w przypadku plików.

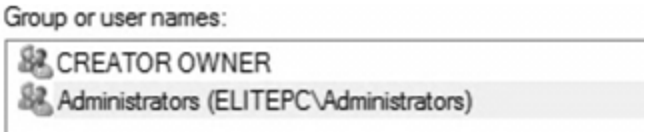


Z posiadaną wiedzą i dwa razy zainstalowaną tą samą drukarką można wdrożyć pewną ciekawą funkcjonalność. Należy wejść we właściwości drukarki szefa. W jej

właściwościach ustawia się priorytet na większy niż był wcześniej, czyli np. 50.



W zabezpieczeniach zostawia się jedynie administratorów (zakłada się, że szef jest administratorem) oraz twórców-właścicieli.



Dla drukarki pracowników można zrobić dokładnie to samo, z tym, że im można ustawić niższy priorytet, np. 10.

Teraz na każdym komputerze szefa należy zainstalować drukarkę, używając tej o wyższym priorytecie, a na innych komputerach tej o niższym. Oba sterowniki odnoszą się fizycznie do tego samego urządzenia, dzięki czemu wydruki szefa są ważniejsze. Gdy szef zapragnie coś wydrukować, wydruki pracowników zostaną wstrzymane na tak długo, aż szef skończy drukować.

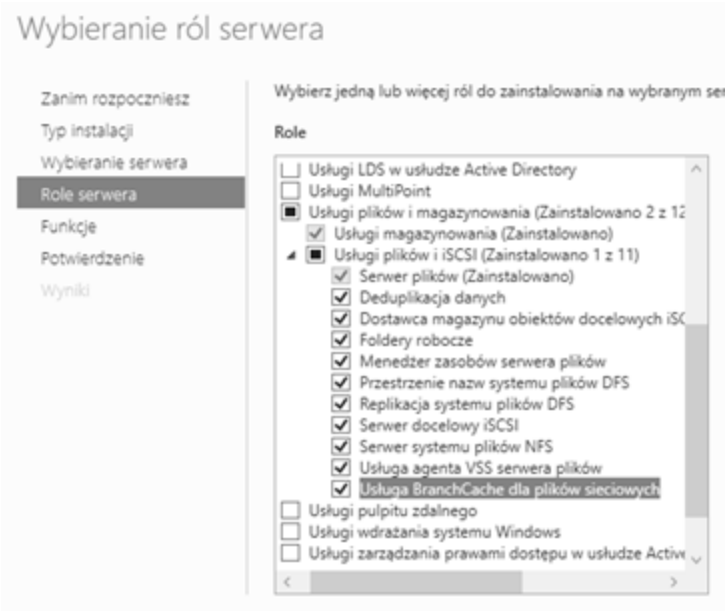
11. Serwer Plików

Serwer plików stanowi najbardziej potrzebną rolę serwera. Służy on nie tylko do scentralizowanego zarządzania danymi i dostępem do nich, ale także dba o bezpieczeństwo danych. Wiążą się z nim takie pojęcia jak

rozproszony system plików, czy klastry, lecz w tym ćwiczeniu zajęto się jego podstawowymi właściwościami.

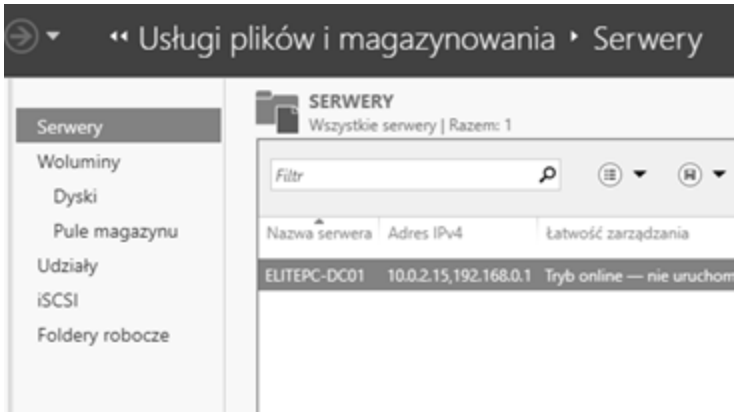
11.1. Instalacja roli Serwera Plików

Należy zatem wejść do kreatora dodawania ról i dodać składniki serwera plików, które nie zostały jeszcze zainstalowane. Część z nich (Storage Pool, Volumes, Shares, iSCSI Virtual Disks) standardowo jest zainstalowana, ponieważ nawet prosta funkcjonalność, jak udostępnianie plików, tego wymaga. Należy wybrać wszystkie brakujące składniki i kliknąć w Dalej (Next).

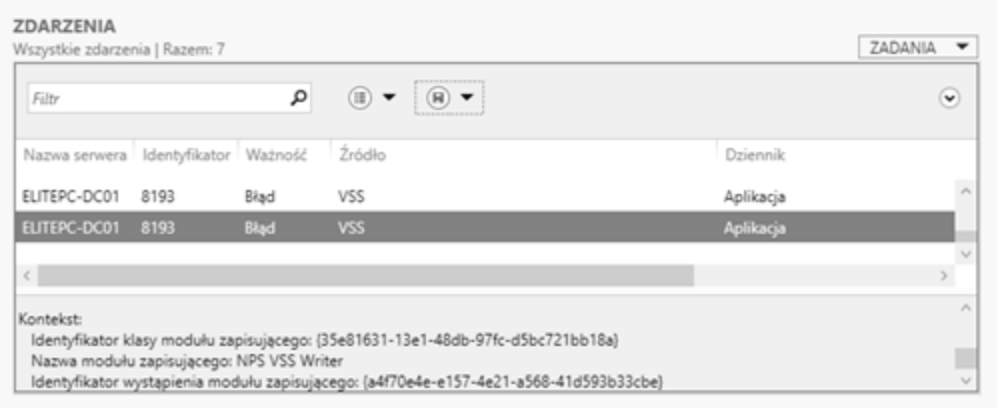


11.2. Zapoznanie z nowym podejściem do usług plików

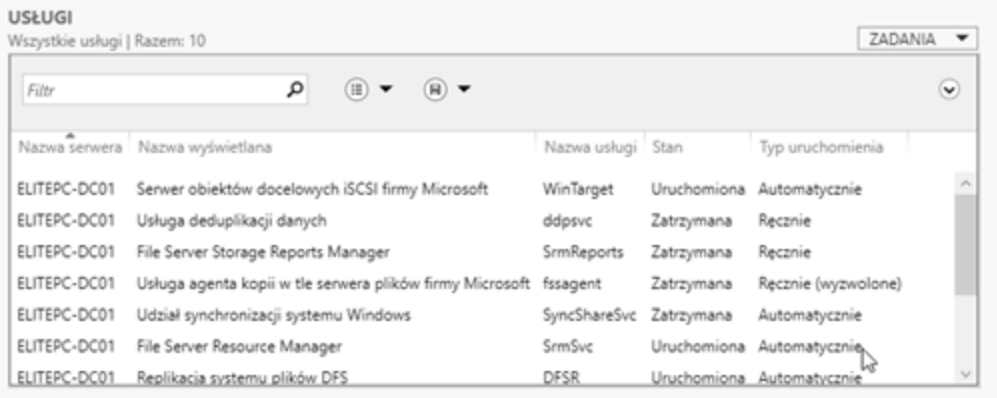
Po instalacji w Menadżerze Serwera (Server Manager) pojawi się nowy wpis: Usługi plików (Files and Storage Services). Po jego zaznaczeniu i wybraniu opcji Serwery (Servers) można dostać się do głównej konsoli zarządzania serwerami plików. W sekcji Serwery (Servers) widać listę serwerów i można nimi zarządzać.



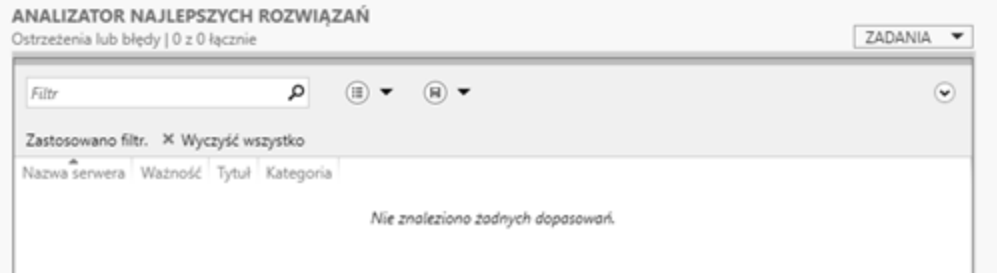
Przesuwając ekran coraz niżej, łatwo znaleźć sekcję Zdarzenia (Events), która loguje i wypisuje zdarzenia, jakie zaszły na serwerze. Używając pobliskiego przycisku Zadania (Tasks), można zdefiniować, jakiego rodzaju zdarzenia są istotne. Do wyboru są: Błędy krytyczne (Critical), Błędy zwyczajne (Error), Ostrzeżenia (Warning) oraz Informacje (Informational). Można też określić, z jakiego przedziału czasu zdarzenia mają być prezentowane.



Jeszcze niżej znajduje się sekcja Usługi (Services). Są to usługi powiązane z serwerem plików, administrator może z tego poziomu podejrzeć, co się z nimi dzieje i uruchomić je ponownie.



Poniżej znajduje się opcja Best Practices Analyzer, która sprawdza konfigurację serwera plików i wyświetla porady dotyczące ewentualnych zmian w jego konfiguracji. Pod guzikiem Zadania (Tasks) kryje się opcja BPA Scan, która przeanalizuje wybrany przez administratora serwer.

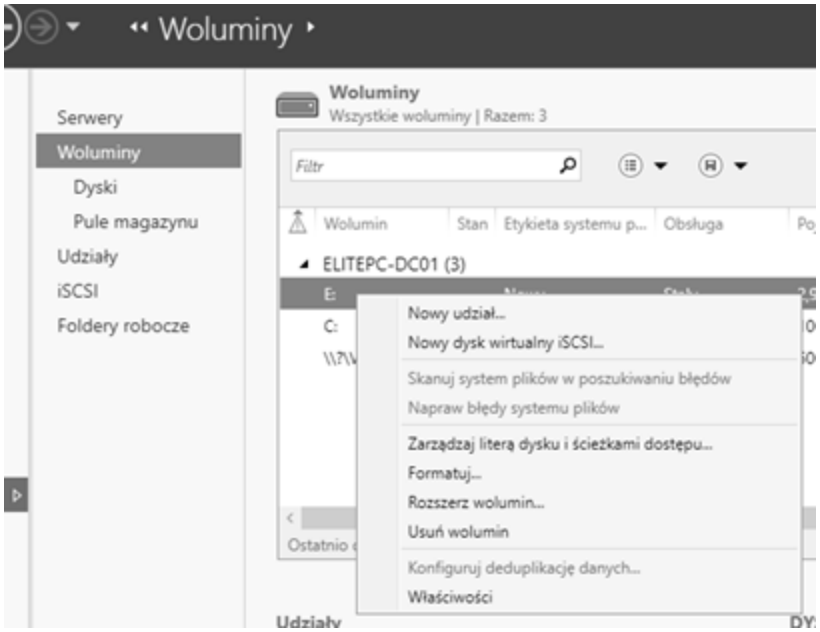


W sekcji Wydajność (Performance) znajduje się Monitor Wydajności (Performance Monitor). Do jego funkcjonalności zalicza się tworzenie alertów wydajności opcją Konfiguruj Alerty Wydajności (Configure Performance Alerts).

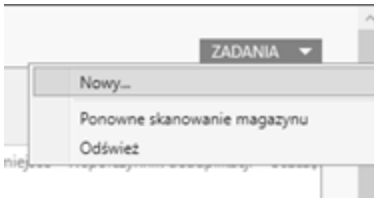
Na samym dole okna znajduje się sekcja Roles and Features gdzie wypisane są składniki serwera plików, jakie funkcjonują na nim. Wśród ról można znaleźć m.in. elementy, które wcześniej zostały już zainstalowane, tj. File Server, który w systemie Windows odpowiada za udostępnianie plików w sieci, BranchCache for Network Files, czyli sieciowe buforowanie plików za pomocą technologii BranchCache, Data Duplication, który skanuje dyski twarde w poszukiwaniu duplikatów plików po to, aby je skasować, DFS Name Spaces, DFS Replication odpowiedzialna za replikację danych pomiędzy rozproszonymi serwerami, File Server Resource Manager będącą przystawką do bardziej zaawansowanego zarządzania udziałami, File Server VSS Agent Service, czyli agent niezbędny do archiwizacji używanych plików przez inne aplikacje, SI Target Server, Server for NFS służący do udostępniania plików komputerów bazujących na Unixie

oraz Storage Service odpowiedzialny za obsługę urządzeń fizycznych.

Po kliknięciu w menu na Woluminy (Volumes) zostanie się przeniesionym do ekranu, w którym ma się podgląd na woluminy istniejące na danym serwerze. Poprzez menu kontekstowe wolumin można naprawić, przeskanować, stworzyć na nim nowy udział, sformatować itp. Jest też podgląd jego podstawowych parametrów, a także, co ważniejsze, w sekcji Udziały (Shares) znajduje się lista wszystkich udziałów sieciowych, jakie się na nim znajdują.



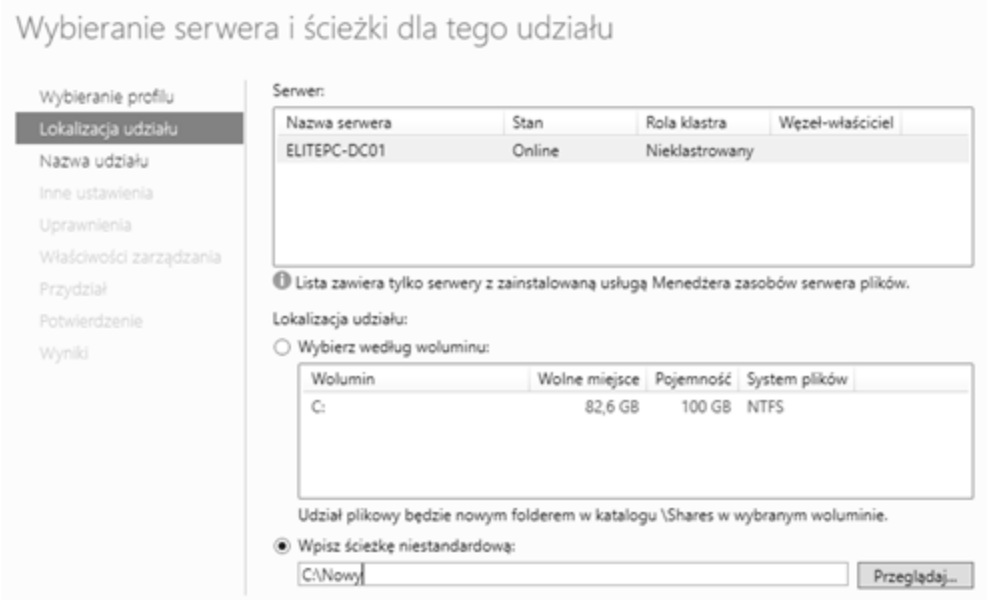
Należy kliknąć w przycisk Nowy udział (New Share) w obrębie sekcji Udziały (Shares).



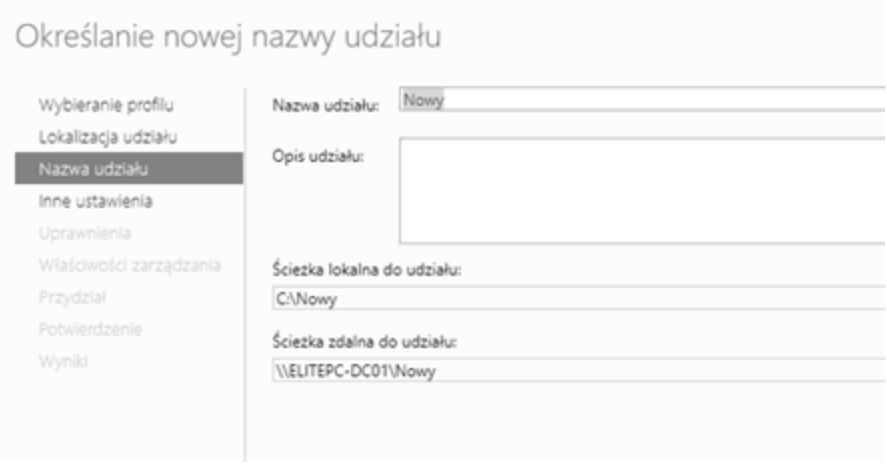
Pojawi się kreator udostępniania, który pozwala wybrać kilka opcji. Te oznaczone przypisem Szybkie (Quick)

pozwalają szybko udostępnić udział protokołem SMB (dla Windows) lub NFS (dla UNIX). Opcje Zaawansowane (advanced) pozwalają dodatkowo w kreatorze zarządzać quotami oraz właściwościami udziału. Istnieje jeszcze udział sieciowy dla aplikacji. Jest on dostosowany do tworzenia udziałów z ustawieniami odpowiednimi dla serwerów aplikacji, serwera Hyper-V czy baz danych. W ramach ćwiczeń zostanie wybrana zaawansowana droga kreatora dla udziału SMB, tj. SMB Share – Advanced.

W kolejnym oknie należy wybrać serwer, na którym dany udział ma zostać utworzony, a także zdefiniować, czy udziałem będzie cały dysk twardy, czy jedynie jakiś folder. W przykładzie poniższym zdecydowano się jedynie na folder.



W następnej kolejności należy określić nazwę dla udziału sieciowego, można zaopatrzyć go w opis, a także konieczne jest zdefiniowanie jego ścieżki sieciowej. Praktycznie wszystkie pola poza opisem domyślnie powinny zostać automatycznie wygenerowane.

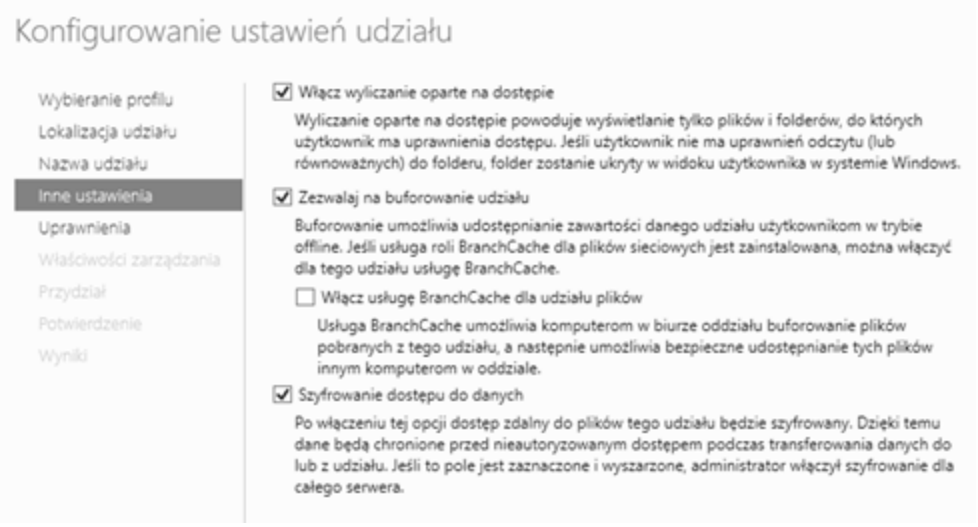


Kolejnym krokiem będzie zdefiniowanie dodatkowych ustawień. Można włączyć Listowanie folderu oparte na uprawnieniach użytkownika (Enable access based enumeration). Rezultat będzie taki, że użytkownik będzie

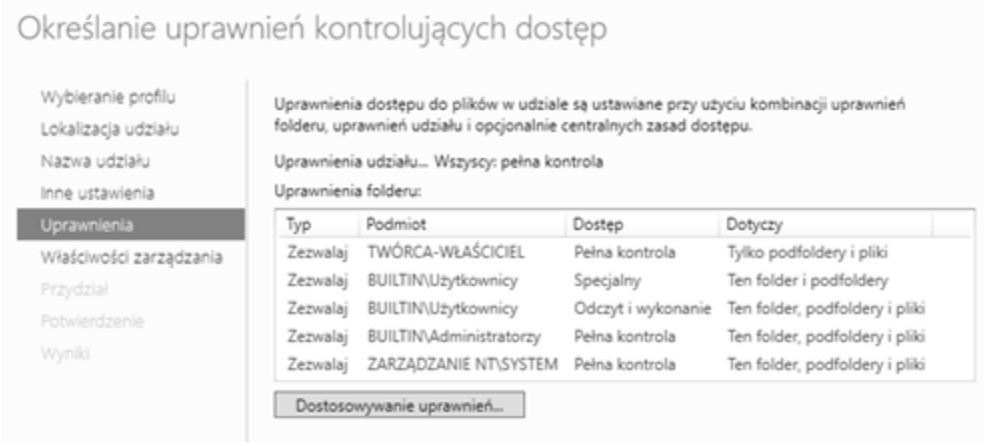
miał wgląd jedynie do tych plików i folderów, do których ma uprawnienia dostępowe.

Opcja Pozwól na buforowanie udziału (Allow Casching of share) pozwoli na buforowanie zawartości udziału sieciowego tak, aby był on dostępny, nawet jeżeli użytkownik jest offline. Dodatkowo można włączyć usługę BranchCache, wymaga ona jednak globalnej dostępności IPv6.

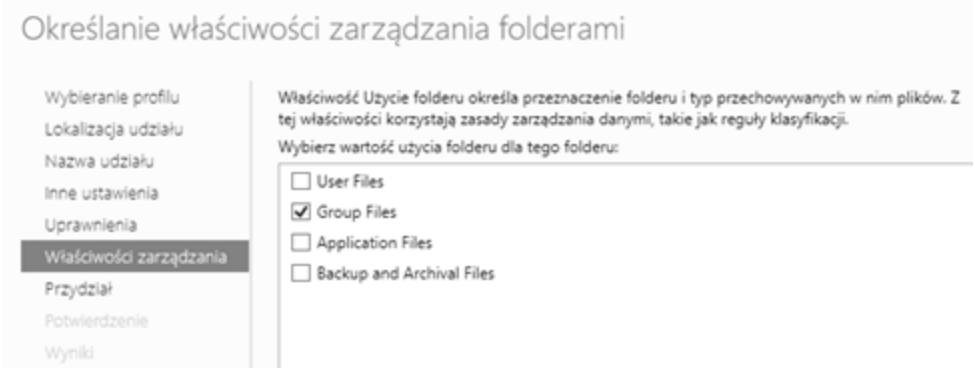
Ostatnią opcją jest Szyfrowany dostęp (Encrypt data access), która to spowoduje szyfrowanie danych podczas połączenia pomiędzy klientem i serwerem w celu uniknięcia przechwycenia danych przez niepowołaną osobę.



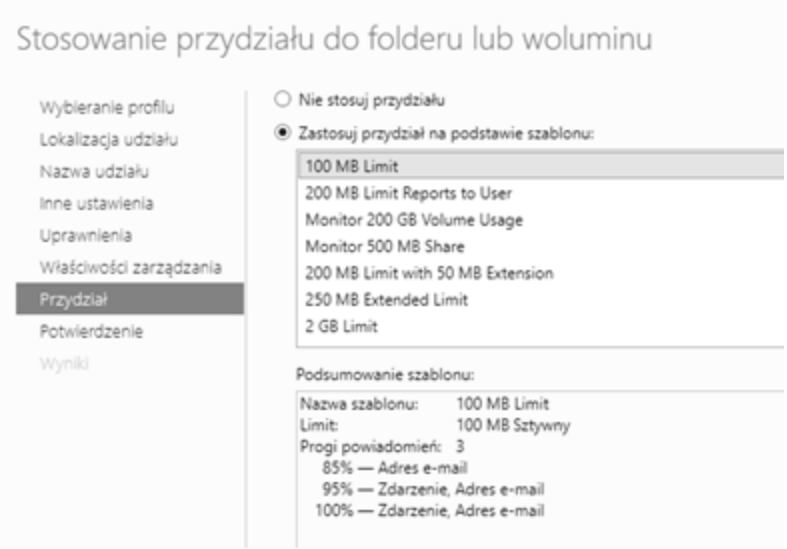
W kolejnym oknie można podejrzeć uprawnienia, jakie będą standardowo przypisane. Przyciskiem Dostosuj uprawnienia (Cuntomize Permisions) łatwo je modyfikować.



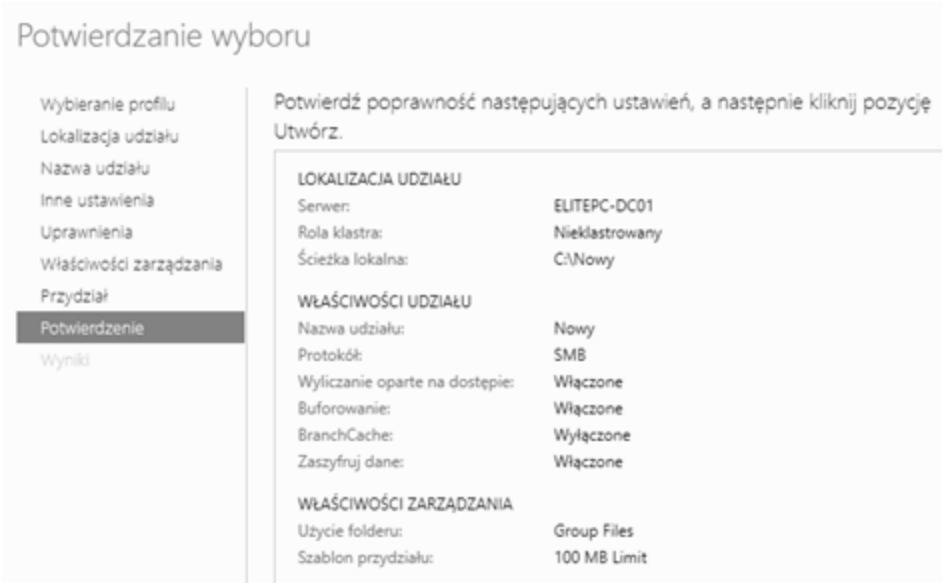
W następnym oknie kreatora należy określić przeznaczenie udziału, czyli to, jakiego rodzaju dane będzie on przechowywał.



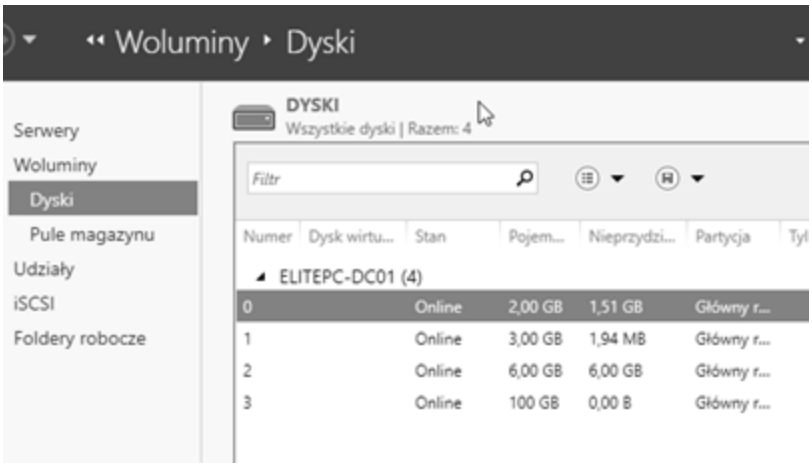
W kolejnym oknie można nałożyć ograniczenie co do ilości danych, jakie ma prawo wgrać użytkownik, czyli tzw. Quoty. Można wybrać dowolną spośród wcześniej zdefiniowanych Quot lub utworzyć nową.



W oknie podsumowania należy kliknąć Utwórz (Create).

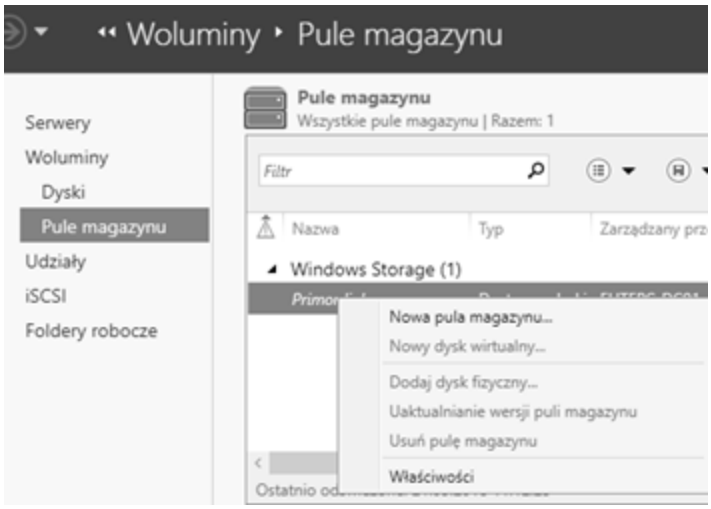


Następnie należy powrócić do widoku Menadżera Serwera (Server Manager) i z Woluminów (Volumes) przejść na Dyski (Disks). Widok jego zawartości jest analogiczny do Woluminów jednak dotyczy już fizycznie całych dysków.



11.3. Storage Pools

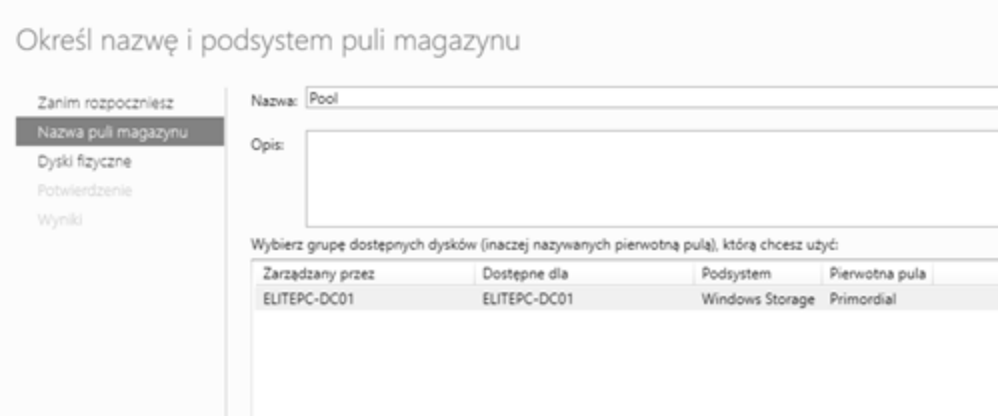
W menu po lewej stronie należy przejść do Storage Pools. Jeżeli komputer spełnia minimalne wymagania sprzętowe, wewnątrz okna powinny być dostępne jakieś urządzenia magazynujące. Po kliknięciu w któreś z nich należy wybrać New Storage Pool.



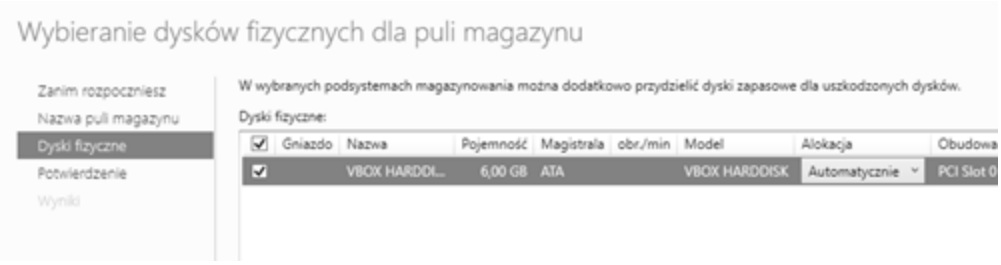
Storage Pools pozwala na połączenie przestrzeni dyskowych relacjami, aby zapewnić zarówno wydajność, jak

i bezpieczeństwo wraz z wysoką dostępnością danych. W ramach ćwiczenia zostanie stworzony jeden wirtualny dysk z kilku fizycznych dysków. Nie może być to używany dysk, na którym zainstalowany jest już system operacyjny, więc wymagany jest przynajmniej jeden odrębny dysk na głównym serwerze lub dwa w przypadku użycia trybu wysokiej dostępności 2-way Mirror, który klonuje zawartość dysku i trzy w trybie 3-way Mirror, gdzie na każdym przechowywana jest kopia danych. Takie dyski powinny być czyste i niesformatowane o rozmiarze minimum 10 GB. Dyski muszą być zainicjowane i online. Mogą być podłączone fizycznie do komputera przez SCSI, iSCSI, SAS czy nawet USB.

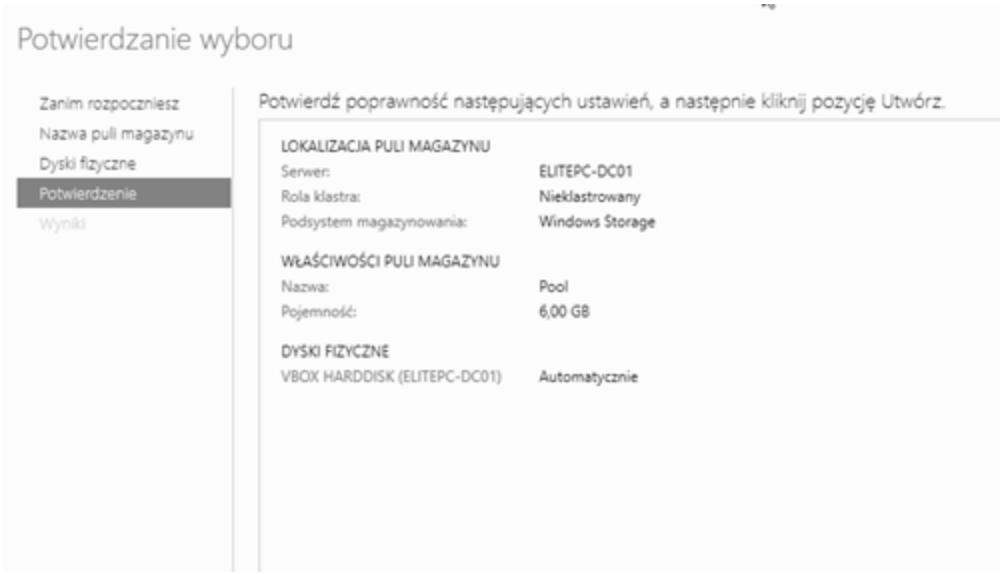
Po pominięciu w kartę powitalną należy wprowadzić nazwę i ewentualnie opis.



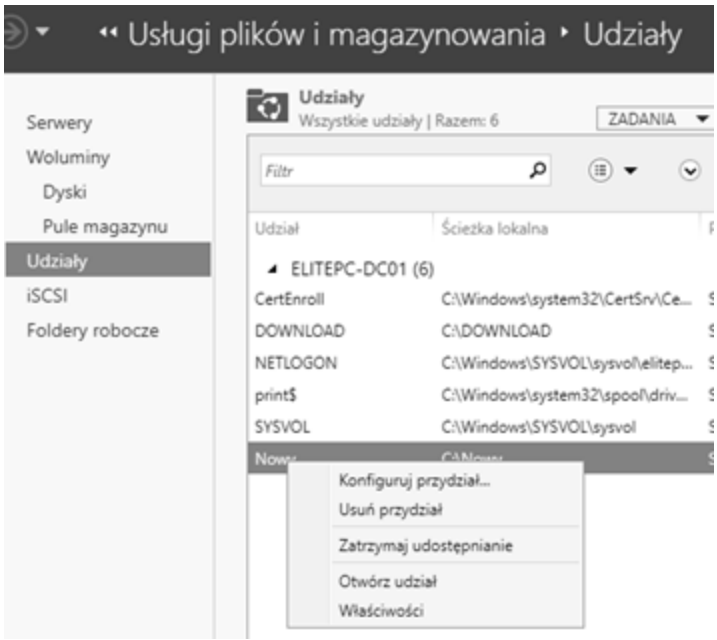
W następnym oknie kreatora zaznacza się dyski, które mają być użyte.



Na koniec należy kliknąć w Utwórz (Create).



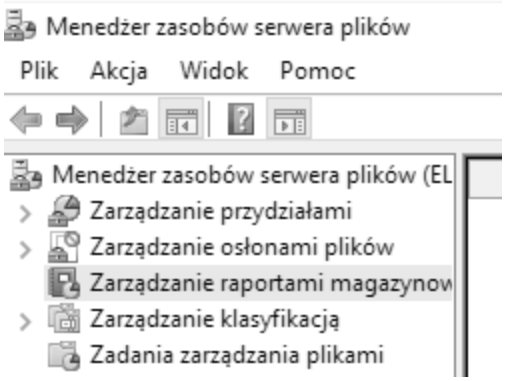
Klikając przycisk Udostępnione (Shares), znajdujący się w menu się po lewej stronie, można przenieść się do widoku, w którym widać będzie wszystkie udziały sieciowe na danym serwerze zebrane w jednym miejscu. W każdej chwili można modyfikować Quoty, wyłączyć udostępnianie czy edytować właściwości udziału.



Powróciwszy do pierwszego okna oznaczonego jako Serwery (Servers) i po kliknięciu prawym przyciskiem myszy na serwerze, należy wybrać File Server Resource Manager.

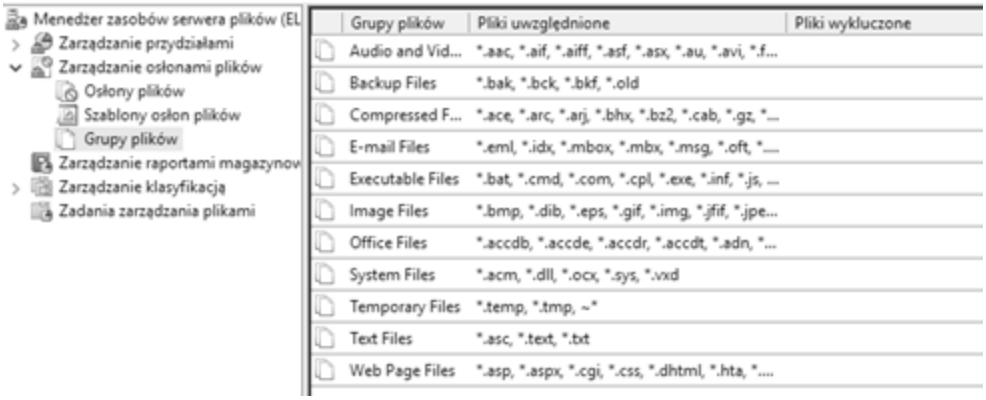
11.4. Zarządzanie przez Menadżera Serwera Plików

Skupiając się na Menadżerze Zasobów Serwera Plików (File Server Resource Manager), raporty o tym, jakie pliki i w jaki sposób były używane można obejrzeć w sekcji Zarządzanie Raportami Magazynowymi (Storage Reports Management).



11.4.1. Zarządzanie Osłonami Plików

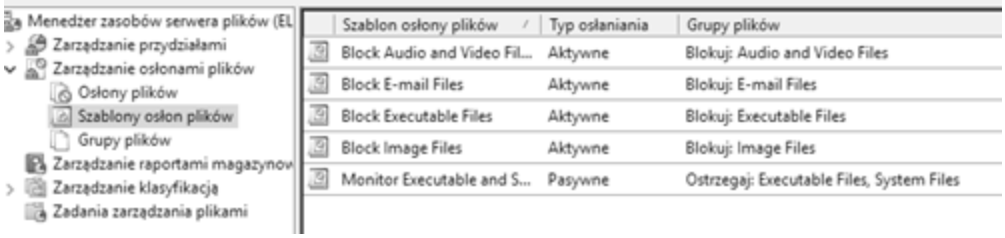
File Screening Management, czyli zarządzanie osłonami plików, pozwala z kolei nie tylko monitorować, ale na przykład zakazywać otwierania jakichś rodzajów plików. W pierwszej kolejności należy utworzyć Grupę plików (File Group). W menu z lewej strony trzeba wybrać Grupy plików (File Groups), a następnie w menu po prawej opcję Utwórz grupę plików (Create File Group).



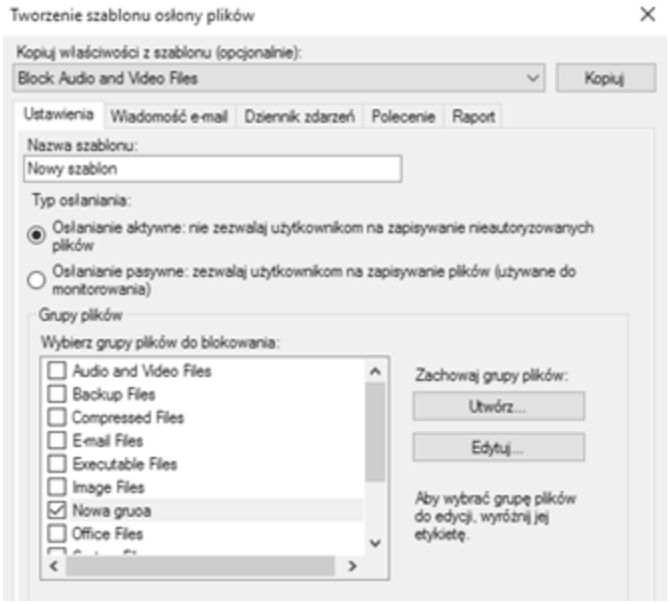
W oknie, jakie się pojawi, należy podać nazwę dla tworzonej grupy plików, a także rozszerzenia plików, jakich będzie ona dotyczyć, w postaci *.rozszerzenie.

Po kliknięciu OK grupa pojawi się na liście.

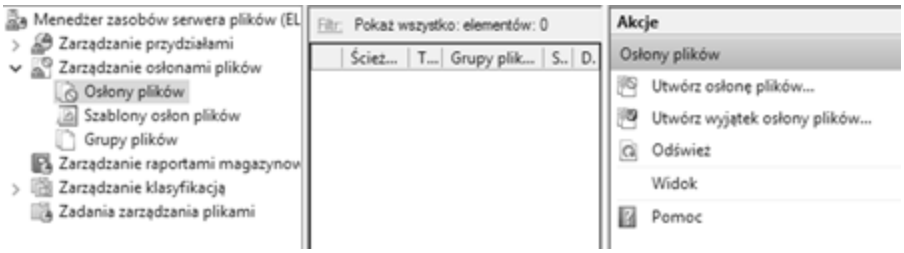
Kolejnym krokiem będzie utworzenie szablonu osłony plików. Należy kliknąć więc na Szablony osłony plików (File Screen Templates) i w menu po prawej stronie wybrać opcję Utwórz szablon osłony plików (Create File Screen Template).



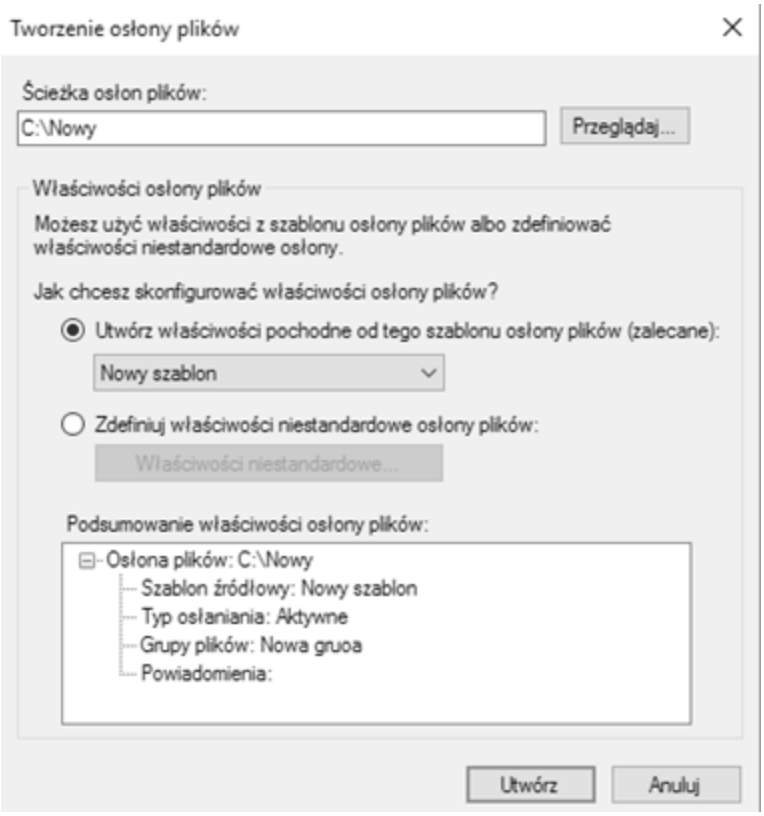
W oknie, które się pojawi, należy zdefiniować nazwę dla szablonu oraz to, czy będzie to osłanianie Aktywne (Active Screening) czy Pasywne (Passive Screening). Aktywne nie pozwoli użytkownikom wgrać do danego folderu określonych przez administratora typów plików, z kolei pasywne pozwoli, lecz wyśle mu informacje o tym, więc będzie służyło bardziej do monitoringu. To, czy zostanie wysłany email z notyfikacją, czy też informacja trafi do logów, definiuje się w zakładkach okna. W ćwiczeniu tym zostanie wybrane osłanianie Aktywne.



Na koniec należy zaznaczyć Osłony Plików (File Screen) i w menu po prawej stronie wybrać Utwórz osłonę plików (Create file Screen).

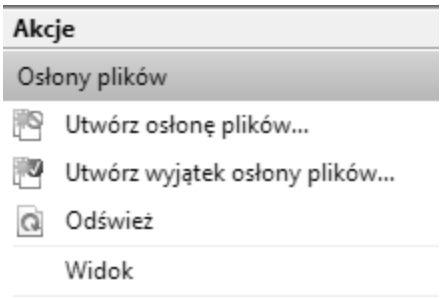


W oknie, jakie się pojawi, wybiera się udostępniony folder, którego ma dotyczyć osłona, oraz osłonę, jaka jest na niego narzucana. Wybór finalizuje się przyciskiem Utwórz (Create).



Od tej pory użytkownicy w wybranym folderze nie będą mieli prawa zapisywania plików o określonych rozszerzeniach. Na dany folder można narzucić kilka różnych osłon, powtarzając kroki, które zostały pokazane powyżej. Wewnątrz danego folderu można także stworzyć wyjątek od osłony, jeżeli w pojedynczym folderze ma

zaistnieć pozwolenie na zapisywanie zabronionych plików, przyciskiem Stwórz wyjątek osłony plików (Create File Screen Exception).



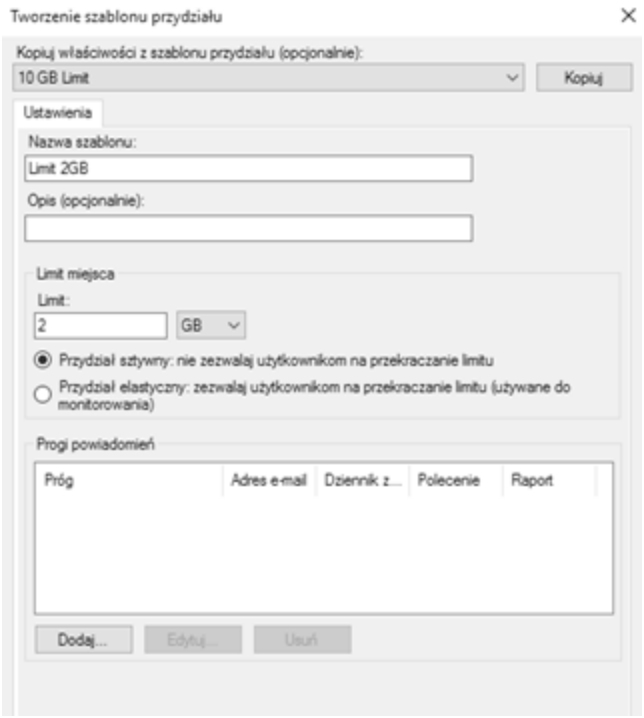
Przykładem z życia wziętym dla zastosowania takiego rozwiązania jest zakazanie włączania plików wykonywalnych, dzięki czemu użytkownicy nie będą w stanie instalować niepożądanych aplikacji.

11.4.2. Zarządzanie Przydziałami

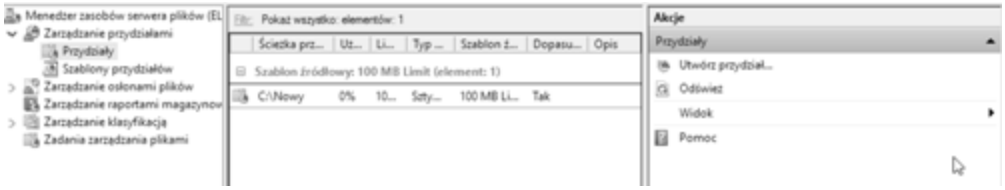
Zarządzanie przydziałami to także bardzo pożyteczna funkcjonalność. Wcześniej został nałożony limit na rozmiar plików użytkownika na dysku. Co jednak, jeśli limit miałby dotyczyć jednego użytkownika albo konkretnego katalogu lub użytkownicy mieliby mieć różne limity? Kilka działów wcześniej został uruchomiony serwer FTP, wypadałoby jednak jakoś ograniczyć użytkownikom powierzchnię dyskową, jaką mogą oni wykorzystać. Tu właśnie można to zrobić. Istnieją oczywiście predefiniowane szablony, są one raczej poglądowe i przykładowe. To są te same szablony,

które kilka stron wcześniej zostały użyte. Aby utworzyć własny szablon, w lewym menu należy rozwinąć Zarządzanie Przydziałami (Quota Management) i kliknąć Szablony Przydziałów (Quota Templates).

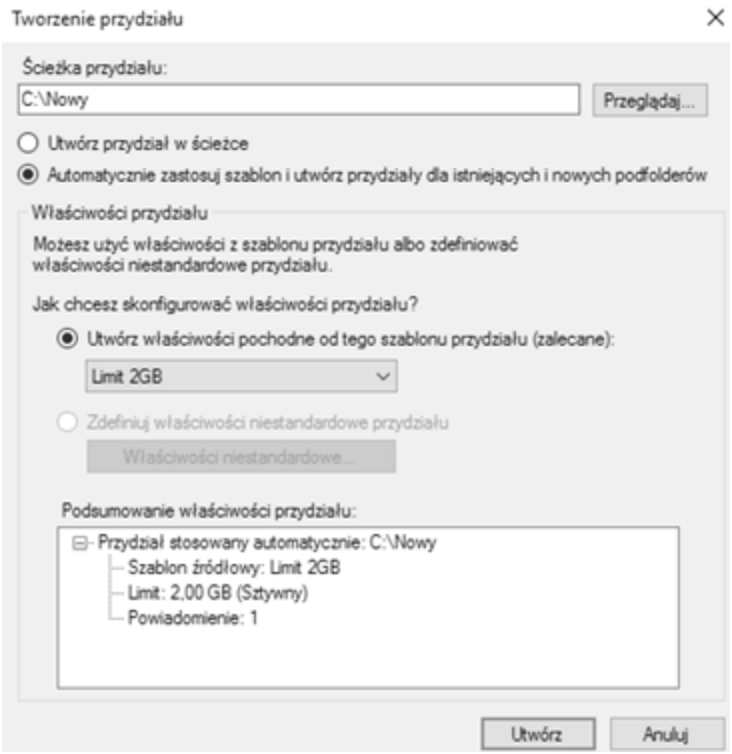
W menu po prawej stronie należy wybrać opcję Utwórz Szablon Przydziału (Create Quota Template). Pojawi się okno, w którym nadaje się szablonowi nazwę, następnie w sekcji Space limit określa się rozmiar dozwolonej pamięci i definiuje, czy przydział będzie Sztywny (Hard Quota) czy Elastyczny (Soft Quota). Pierwszy nie pozwoli wgrać więcej danych niż zakłada limit, drugi pozwoli, lecz będzie komunikował to użytkownikowi. Wybrana zostanie Hard Quota i nadany limit, np. 2 GB.



Z drzewa kategorii z lewej strony należy wybrać Przydziały (Quotas), a następnie po prawej kliknąć w przycisk Utwórz przydział (Create Quota).



Należy wybrać ścieżkę do jakiegoś katalogu z przygotowanego szablonu. Użytkownicy teraz nie będą mogli przechowywać tam więcej danych niż przewiduje limit, np. jeżeli limit wynosi 100 MB, to każdy użytkownik może wgrać maksymalnie 100 MB własnych danych. Warto też zaznaczyć opcję Auto apply template and create quotas on existing and new subfolders, ponieważ dzięki temu przydziały będą również nakładane na nowo tworzone foldery.



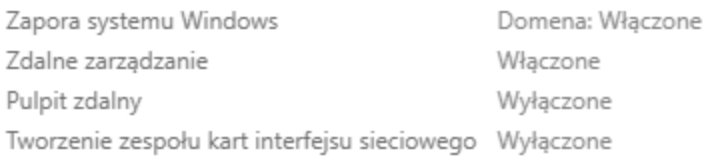
12. Praca zdalna

Serwer powinien dawać administratorowi możliwość zarządzania zdalnego. Dlatego też skonfigurowane zostanie połączenie pulpitu zdalnego. Proces ten jest relatywnie łatwy, a funkcja pulpitu zdalnego dobrze zaimplementowana. Dzieje się tak, ponieważ elementy interfejsu Windows zawierają się już w systemach czy aplikacjach klienckich. Co więcej, klienta dostępu zdalnego Microsoft przygotował także na inne platformy jak Linux, OS X, a nawet urządzenia mobilne, dzięki czemu w awaryjnej sytuacji można odratować serwer nawet przez komórkę, jadąc pociągiem.

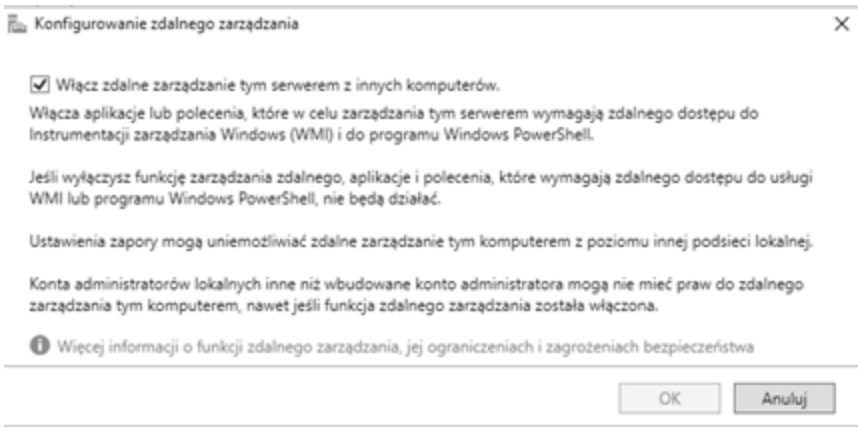
12.1. Wstępna konfiguracja serwera

Należy kliknąć w Serwer Lokalny (Local Server) w Menadżerze Serwera (Server Manager).

Zostanie wybrane i uruchomione Zdalne Zarządzanie (Remote Management) znajdujące się po prawej stronie okna.

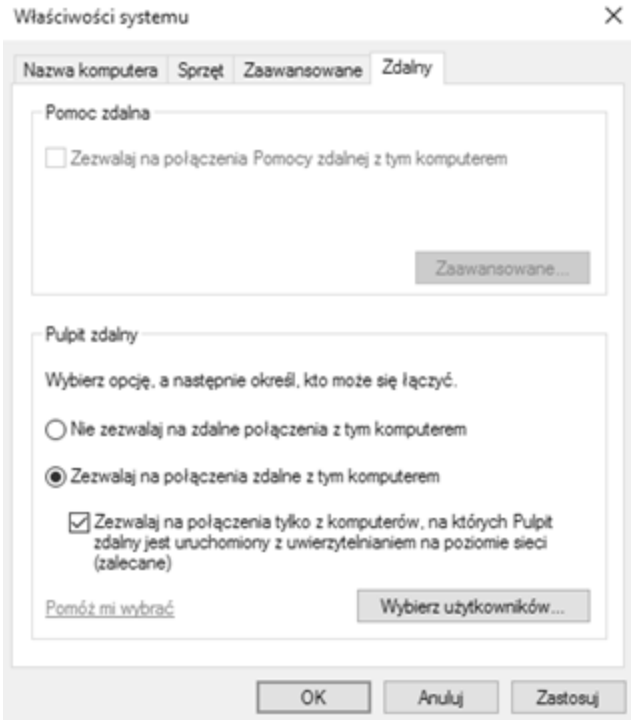


W okienku, które się pojawi, należy zaznaczyć Zezwalaj na zdalne zarządzanie tym serwerem z innych komputerów (Enable remote management of this server from other computers), co pozwoli na zarządzanie tą maszyną choćby przez Menadżera Serwer (Server Manager) uruchomionego na innym komputerze bądź za pomocą PowerShella.

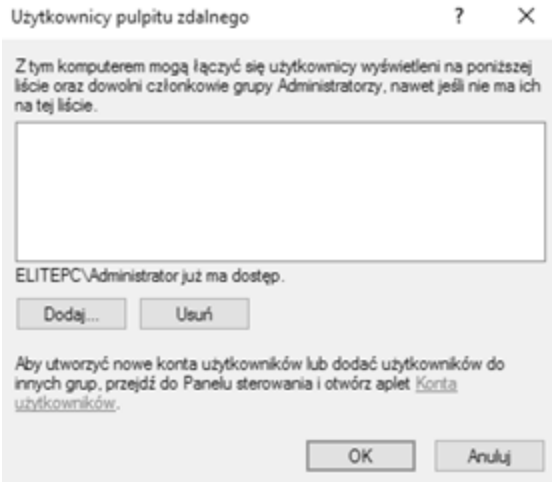


Tuż poniżej należy uruchomić dostęp poprzez połączenie Pulpitu zdalnego (Remote Desktop).

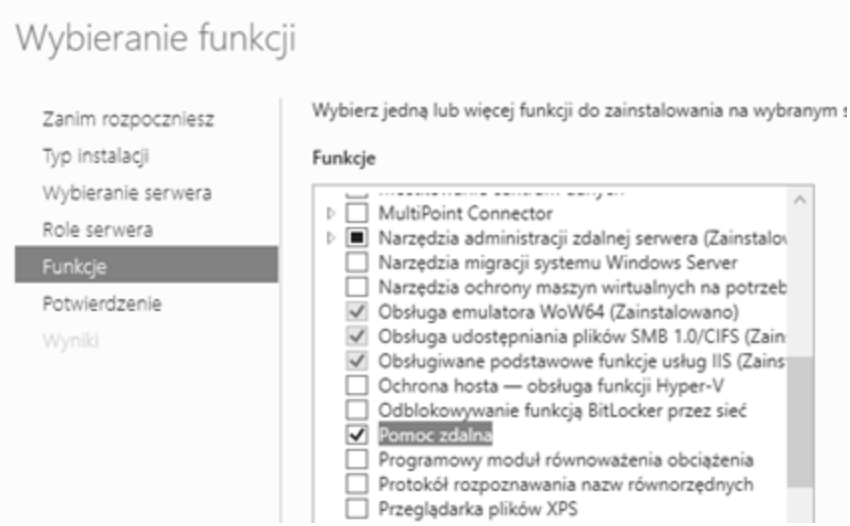
W oknie, które się pojawi, należy wybrać opcję Pozwól na zdalne łączenie z tym komputerem (Allow remote connections to this computer). Można także zaznaczyć zgodę na połączenia zdalne wyłącznie z komputerów, które są zautentykowane na poziomie sieci, co zwiększa bezpieczeństwo.



Kliknąwszy w opcję Wybierz użytkowników (Select Users), można dodać użytkowników, którzy będą mieli możliwość zdalnego łączenia się z tą maszyną. Administratorów nie trzeba tu wprowadzać, ponieważ oni już domyślnie mają stosowne uprawnienia.

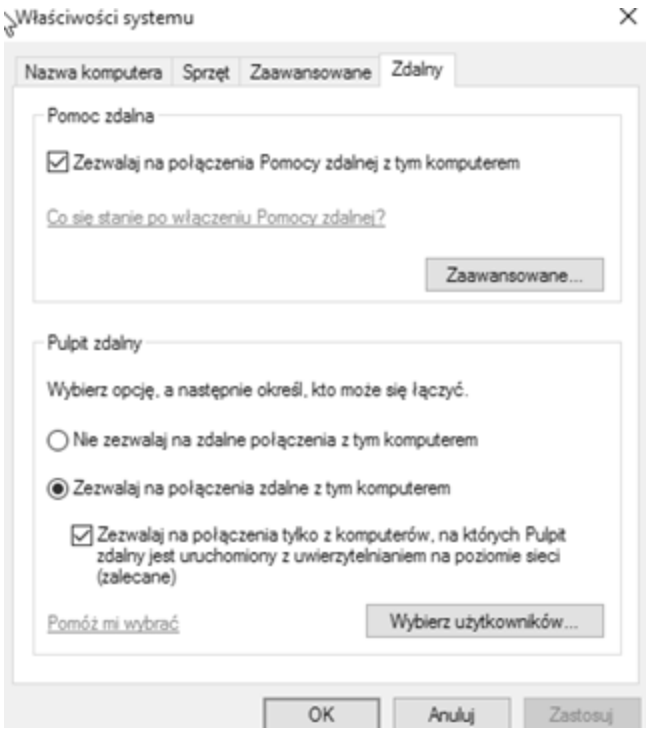


Zanim się przejdzie do konfiguracji klienta i testowania połączenia, warto zainstalować i skonfigurować pomoc zdalną. W pierwszym kroku należy doinstalować funkcję Zdalna Pomoc (Remote Assistance).



Gdy proces instalacji dobiegnie końca, należy wrócić do okna, w którym został uruchomiony Pulpit Zdalny (Remote

Desktop). Teraz będzie możliwość uruchomienia również Zdalnej Pomocy (Remote Assistance). Należy zaznaczyć opcję Zezwól na połączenia zdalnej pomocy z tym komputerem (Allow Remote Assistance connections to this computer).

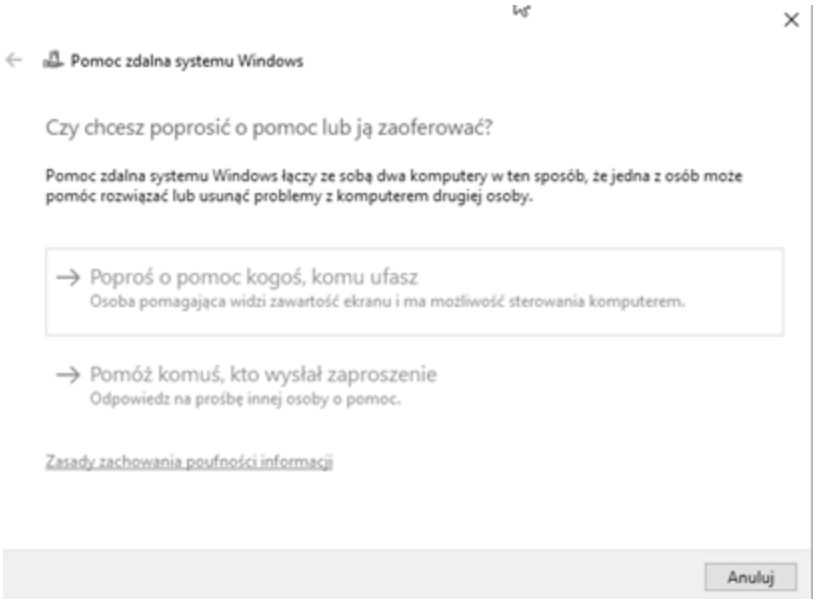


12.2. Korzystanie z Pomocy Zdalnej

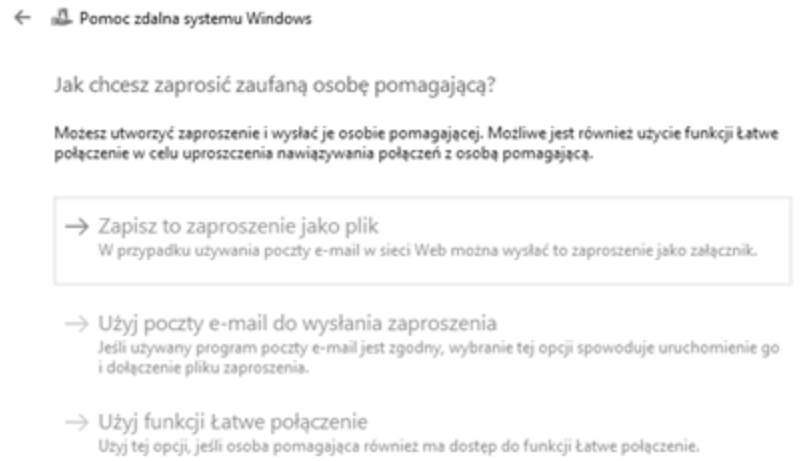
Zanim przystąpi się do prezentacji działania systemu po stronie klienta, należy wysłać zaproszenie do pomocy. W wyszukiwarce dla sekcji Ustawienia (Settings) należy wpisać słowo Zaproś (Invite) i z listy wyników wybrać Zaproś kogoś do połączenia z twoim PC na pomoc tobie, lub zaoferuj swoją pomoc komuś innemu (Invite someone to

connect to your PC and help you, or offer to help someone else) – wyszukaj jako msra.

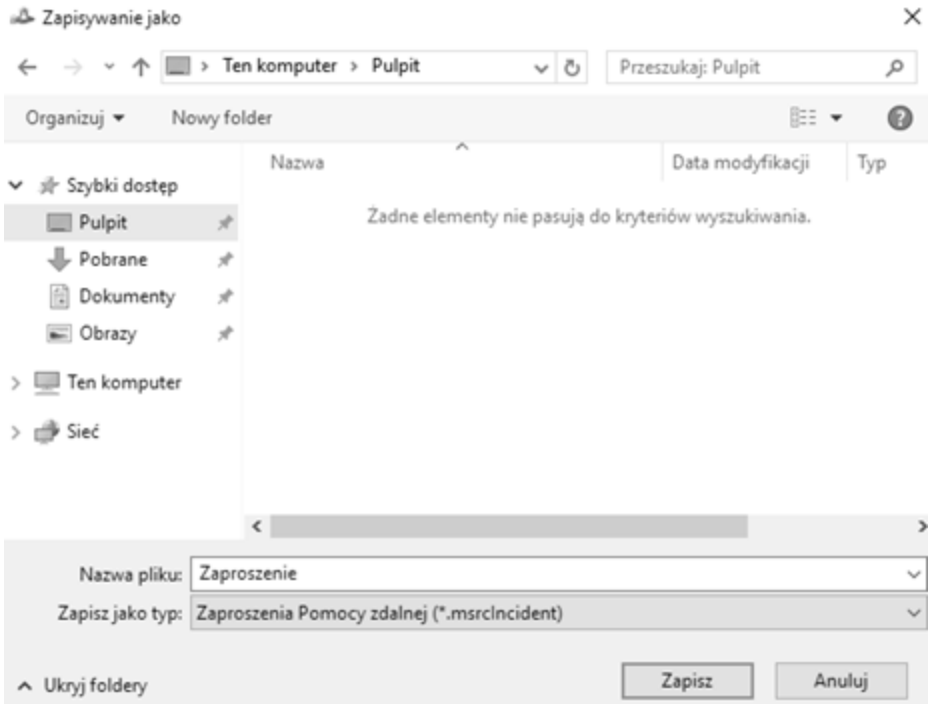
Zostanie otwarte nowe okno, w którym pojawią się dwie opcje. Pierwsza to prośba o pomoc, druga to pomoc innej osobie. Dla przykładu zostanie wybrana opcja pierwsza Zaproś kogoś komu ufasz, żeby ci pomógł (Invite someone you trust to help you).



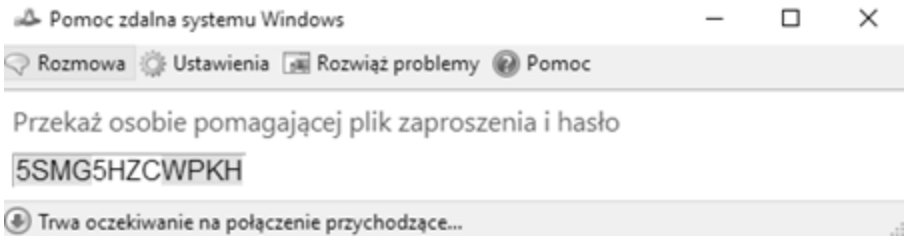
Należy kliknąć przycisk Poproś kogoś komu ufasz o pomoc (Invite someone you trust to help you) znajdujący się w centrum ekranu. Pojawią się trzy opcje. Jedna z nich to stworzenie odpowiedniego pliku z danymi, który trzeba dostarczyć we własnym zakresie danej osobie (Save this invitation as file), kolejna opcja to zaproszenie poprzez e-mail (Use email to sen dan invitation), a ostatnia opcja to łatwe połączenie (Use easy connect).



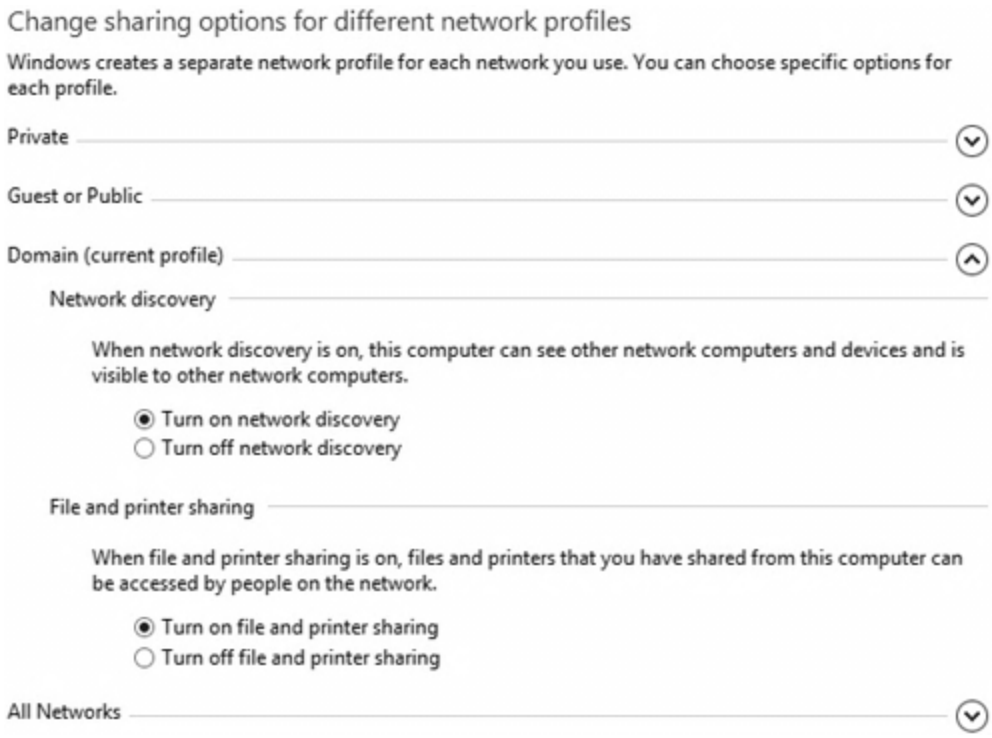
Najwygodniej będzie oczywiście to zrobić, zapisując zaproszenie jako plik. Potem należy go udostępnić w sieci – w przypadku książkowym zostanie użyty komputer zdalny.



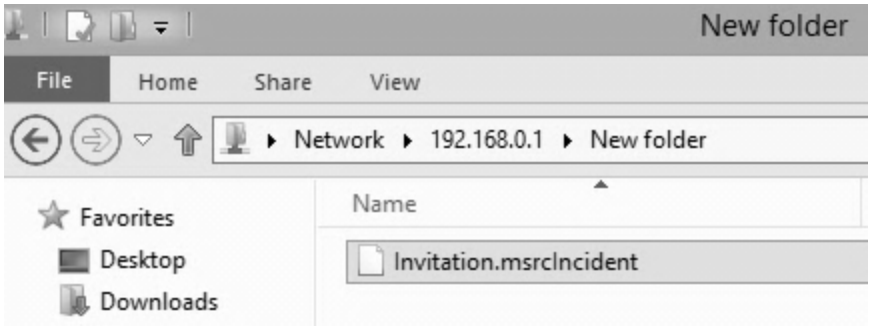
Wygenerowane zostanie hasło, które trzeba ręcznie przekazać osobie, mającej udzielić pomocy.



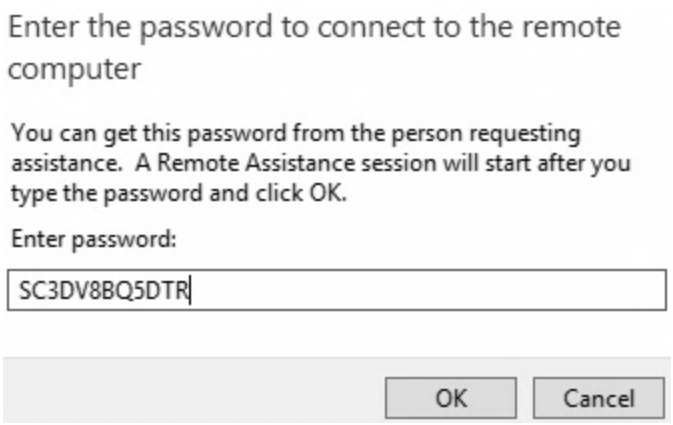
Jeśli nie zostało to wcześniej zrobione, aby można było odnaleźć komputer w sieci, należy na serwerze wprowadzić poniższe ustawienia.



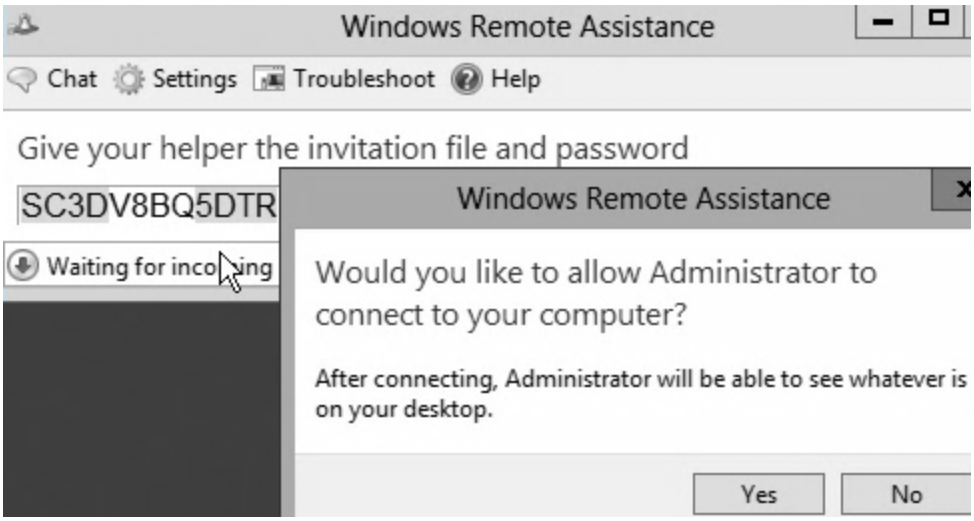
Należy udostępnić w sieci plik z zaproszeniem, a następnie wejść do udostępnionego folderu z drugiego komputera.



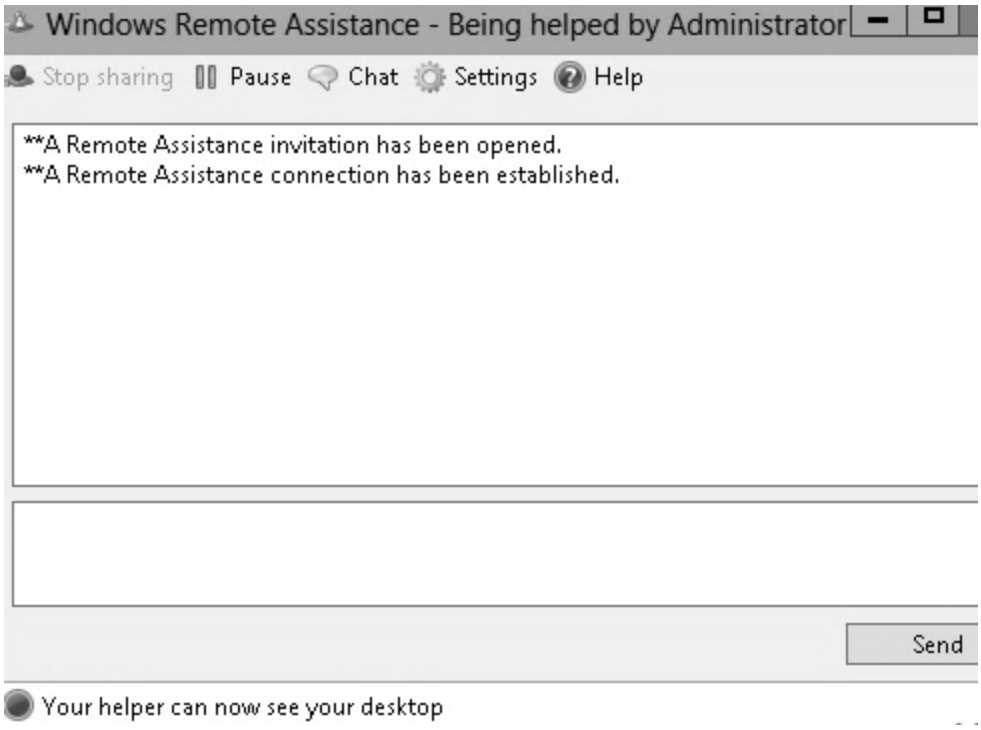
Później należy wybrać udostępnione wcześniej zaproszenie i uruchomić je podwójnym kliknięciem. Trzeba pamiętać o tym, że na zdalnym komputerze musi być zainstalowana funkcja zdalnej pomocy. Konieczne będzie także wprowadzenie wygenerowanego na serwerze hasła.



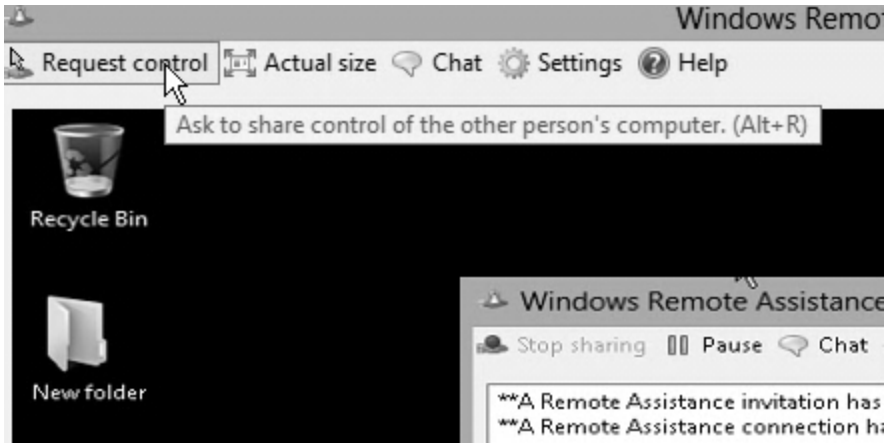
W tej chwili na komputerze nadawcy pojawi się komunikat, który należy potwierdzić, klikając w Tak (Yes); dopóki nie zostanie to zrobione, osoba pomagająca nie będzie w stanie nic zrobić.



Na komputerze, który potrzebuje pomocy, pojawi się okienko czatu, dzięki któremu można rozmawiać z pomocnikiem itp.

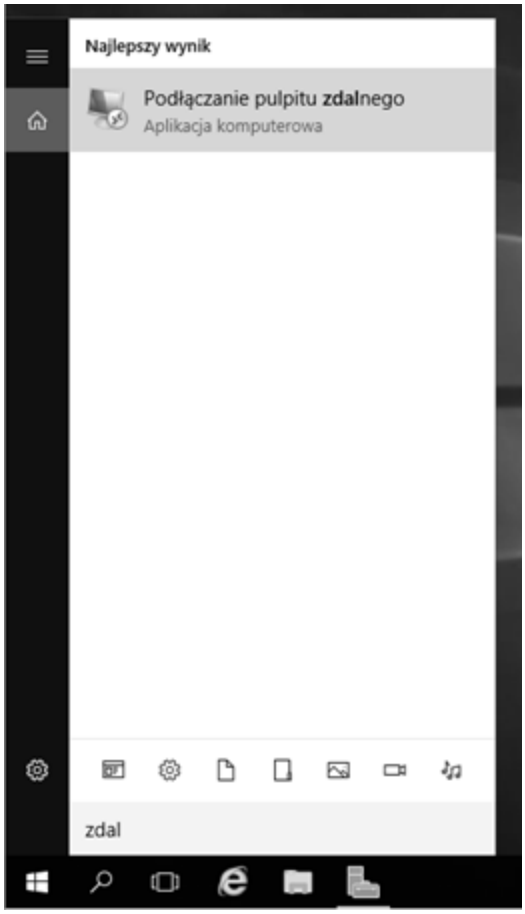


Obie strony pracują jednocześnie na jednym pulpicie i widzą go, w związku z czym pomocnik może albo nauczyć czegoś drugą osobę, wydając jej polecenia i patrząc jak je realizuje, lub po prostu przejąć kontrolę nad komputerem, do którego się podłączył i samemu wykonać powierzone zadanie.



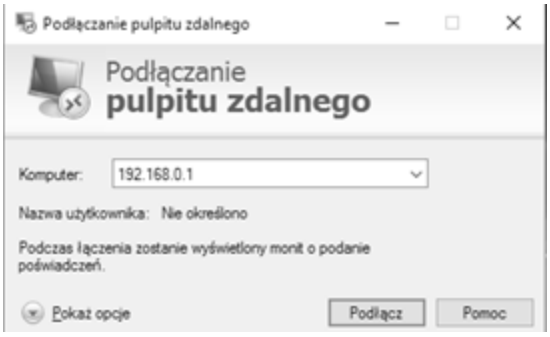
12.3. Nawiązywanie połączenia pulpitu zdalnego

W tym poddziale zostanie nawiązane połączenie z serwerem za pomocą Pulpitu Zdalnego (Remote Desktop). Należy wyszukać program Połączenie Pulpitu Zdalnego (Remote Desktop Connection), a następnie go uruchomić.

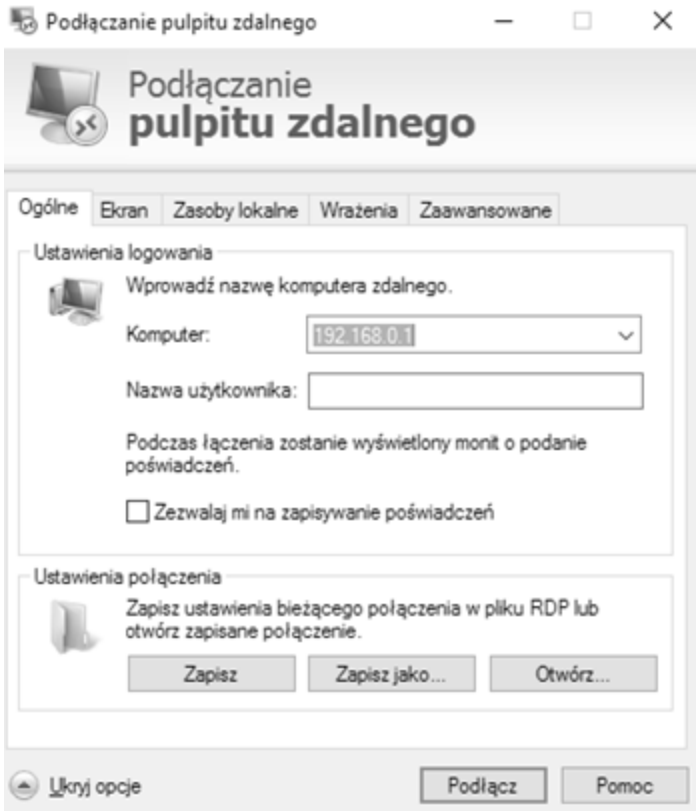


Pojawi się małe okno dialogowe, w którym de facto wystarczy podać adres serwera. Nie ważne czy będzie to adres IP, czy nazwa domeny ,np. elitepc.pl. Będąc

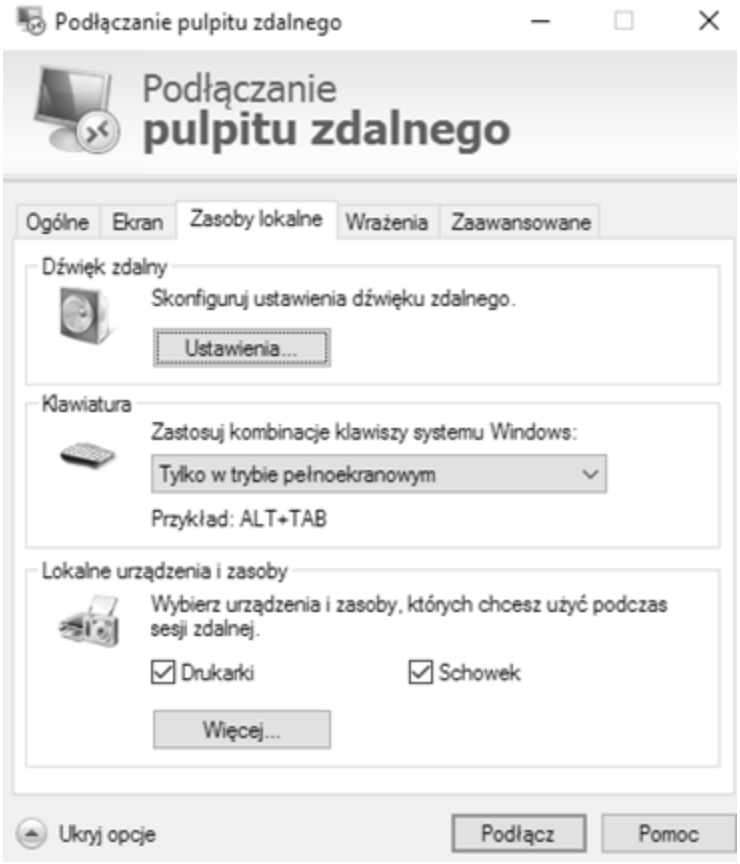
w domenie, można po prostu wpisać nazwę komputera docelowego.



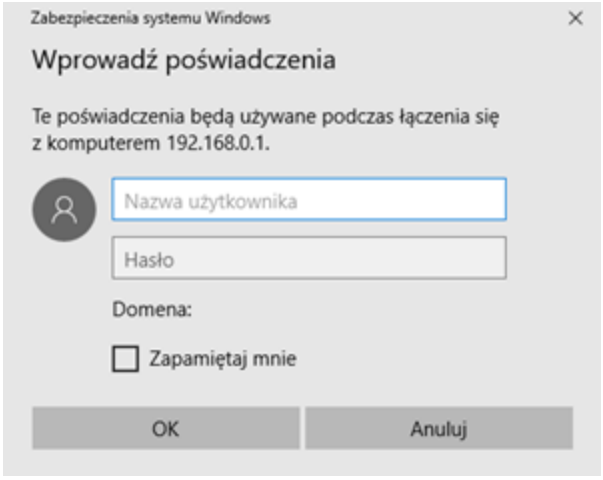
Przed połączeniem warto także rozwinąć opcje przyciskiem Pokaż Opcje (Show Options). Między innymi znajduje się tam możliwość zapisania ustawień połączenia pulpitu zdalnego w formie pliku, dzięki czemu następnym razem wystarczy kliknąć, aby zdalnie połączyć się z serwerem.



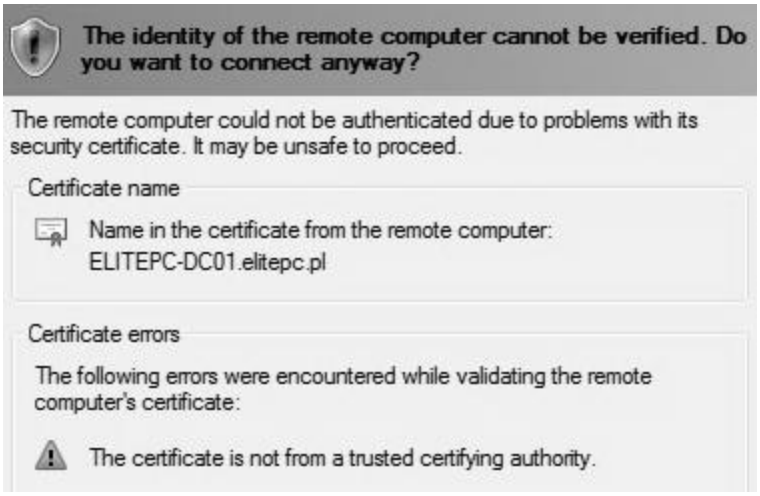
W zakładce Zasoby lokalne (Local Resources) znajdują się opcje związane z dostępem do zasobów lokalnych. Na komputerze zdalnym będzie można między innymi przenieść dźwięk, skróty klawiaturowe, zawartość schowka, drukarki czy inne urządzenia Plug and Play.



Po kliknięciu w Podłącz (Connect) należy zalogować się do komputera docelowego. Konieczne będzie podanie danych do logowania.



Należy potwierdzić certyfikat. Jest to krok niezbędny, ponieważ połączenie z pulpitem zdalnym ze względów bezpieczeństwa musi być szyfrowane.



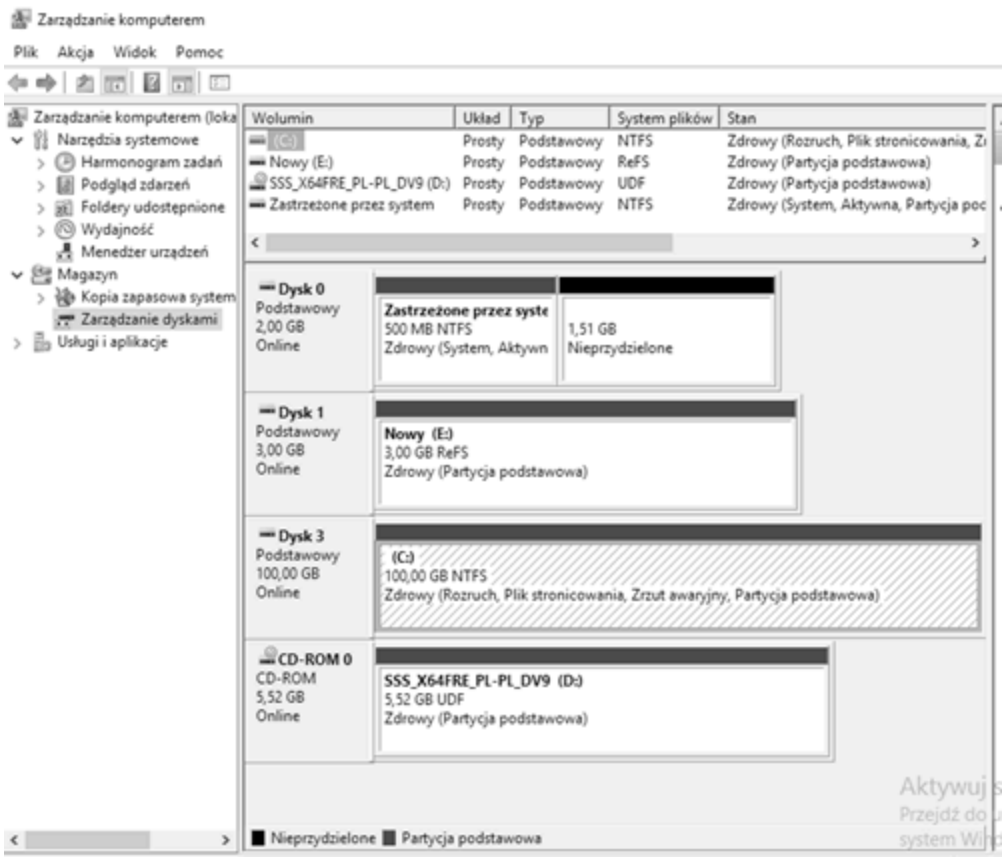
Połączenie powinno zostać nawiązane. Ten sposób logowania na serwerze pozwala na taką na nim pracę, jak gdyby administrator pracował bezpośrednio na nim. Pracę w trybie zdalnym można rozpoznać po dodatkowym pasku na górze ekranu.

13. Zarządzanie dyskami

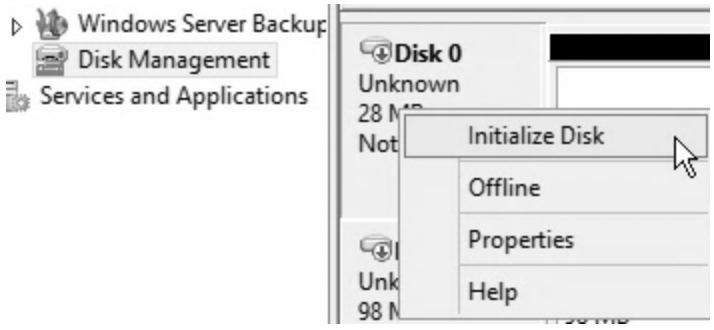
W systemie Windows Server 2016 można przekonwertować dyski na tak zwane dyski dynamiczne, które oferują zwiększone możliwości. Dyski dynamiczne zapewniają funkcje niedostępne na dyskach podstawowych, takie jak możliwość tworzenia woluminów obejmujących wiele dysków (woluminy łączone i rozłożone) czy odpornych na uszkodzenia (woluminy dublowane i RAID-5). Wszystkie woluminy na dyskach dynamicznych są nazywane woluminami dynamicznymi. Istnieje pięć typów woluminów dynamicznych: proste, łączone, rozłożone, dublowane i RAID-5. Woluminy dublowane i RAID-5 cechują się odpornością na uszkodzenia i są dostępne wyłącznie na komputerach z systemem Windows 2000 Server, Windows 2000 Advanced Server, Windows2000 Datacenter Server lub z systemami operacyjnymi Windows Server2003 i nowszych. Za pomocą komputera z systemem Windows 7 Professional można jednak zdalnie tworzyć woluminy dublowane na komputerach z tymi systemami operacyjnymi. Bez względu na to, czy używanym stylem partycjonowania dysku dynamicznego jest główny rekord rozruchowy (MBR), czy tabela partycji GUID (GPT), można utworzyć nawet 2000 woluminów dynamicznych. Zalecana liczba woluminów dynamicznych to 32 lub mniej.

Należy więc wejść do Konsoli zarządzania komputerem (Computer Management).

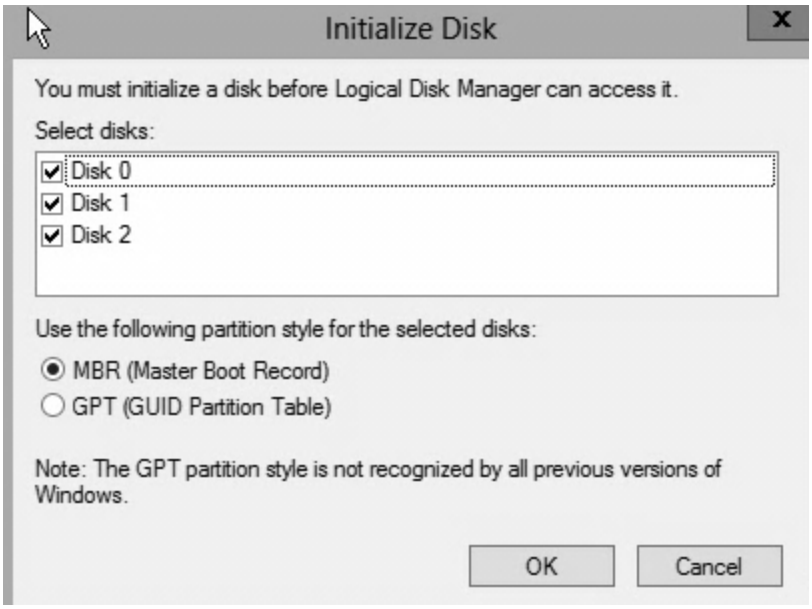
Potem kliknąć w Zarządzanie dyskami (Disk Management). Po prawej stronie pojawi się lista partycji, a pod nią lista fizycznie podłączonych do komputera dysków. Jak widać, są to trzy dyski, o których wspomniano w dziale opisującym środowisko, w którym Windows Server 2016 został zainstalowany. Nie były one jeszcze ani formatowane, ani inicjalizowane.



Teraz na wybranym nieaktywnym dysku należy kliknąć w Zainicjuj dysk (Initialize Disk), po to, aby zaczął działać.

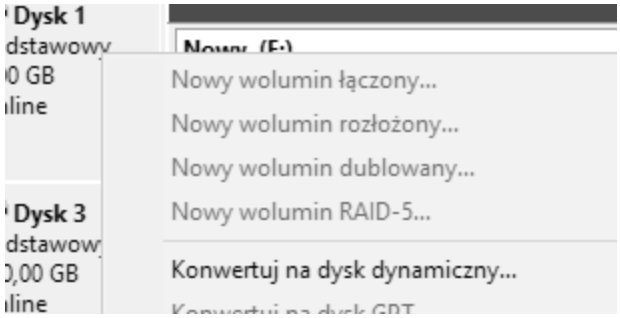


Należy pamiętać, że inicjowanie jest nieodwracalne. W oknie, które się pojawi, trzeba wybrać wszystkie dyski twarde i kliknąć OK. Warto zauważyć, że drzewo partycji, jakie zostanie na nim utworzone, może być typu zarówno MBR,jak i nowego typu GUID. Dla systemów Windows standardem jest MBR.

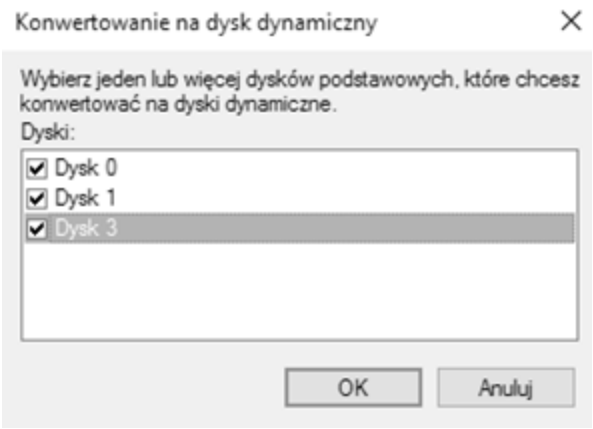


Należy przekonwertować dyski na dyski dynamiczne. Dzięki temu zyskuje się możliwość ich zaawansowanych ustawień i tworzenia macierzy dyskowych. Trzeba jednak pamiętać, że ponieważ macierze nie są sprzętowe, lecz programowe, będą wolniejsze od sprzętowych. Co więcej, dysku skonwertowanego na dynamiczny nie uda się bez problemów odczytać na innym komputerze.

Na wybranym dysku należy kliknąć prawym przyciskiem myszy i wybrać opcję Konwertuj dysk na dynamiczny (Convert to Dynamic Disk).

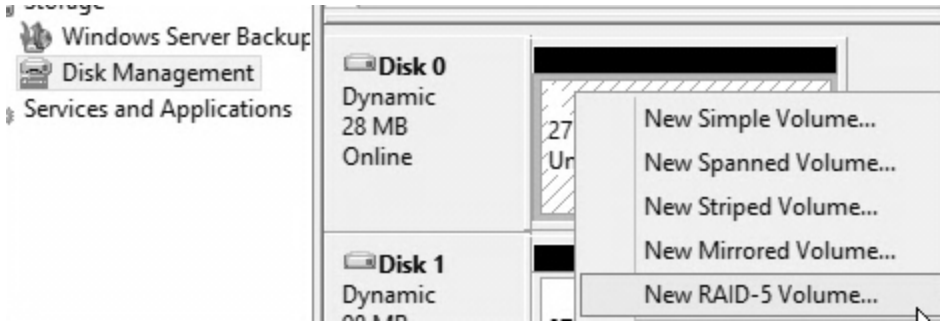


W oknie, które się pojawi, należy wybrać dyski. Zostaną wybrane tylko trzy dodatkowe dyski służące ćwiczeniu, a wybór zostanie potwierdzony kliknięciem OK.

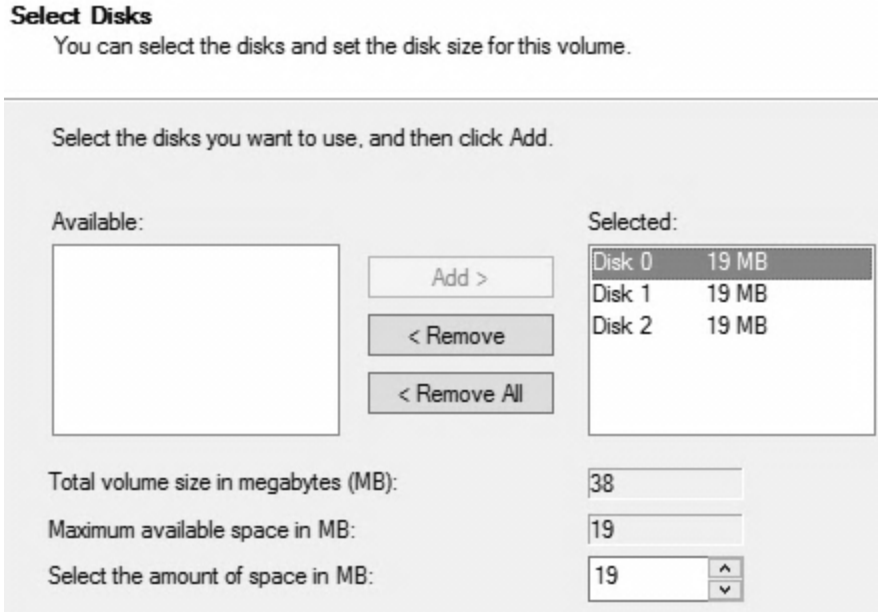


Teraz, klikając w wybrany dysk prawym przyciskiem myszy, można utworzyć jeden z pięciu woluminów. Wolumin prosty (Simple Volume) jest odpowiednikiem zwyczajnej partycji, z tym, że w przyszłości będzie można swobodnie modyfikować jego rozmiar, jeżeli pozwoli na to dysk twardy. Wolumin łączony (Spanned Volume) pozwala połączyć ze sobą kilka dysków twardych w jeden duży, a jego zaletą jest to, że dyski mogą mieć różne rozmiary. Nie daje on żadnego przyrostu szybkości pracy dysków ani bezpieczeństwa przed utratą danych. Wolumin rozłożony (Stripped Volume) z kolei jest alternatywą dla RAID 0. Łączy on dwa dyski o identycznej pojemności i zapisując jednocześnie na obu z nich fragmenty danych, sprawia, iż dysk działa szybciej. Wolumin dublowany (Mirrored Volume) łączy dwa dyski ze sobą w taki sposób, że na jednym z nich przechowywana jest kopia drugiego, podobnie jak w RAID 1. Dla przykładu zostanie stworzony nowy wolumin RAID 5. Stanowi on jakby połączenie RAID 0 i RAID 1. Wymaga co najmniej trzech dysków. Dwa z nich łączone są tak, jak w przypadku woluminu rozłożonego, natomiast trzeci dysk przechowuje część danych uzyskaną przez operację arytmetyczną XOR.

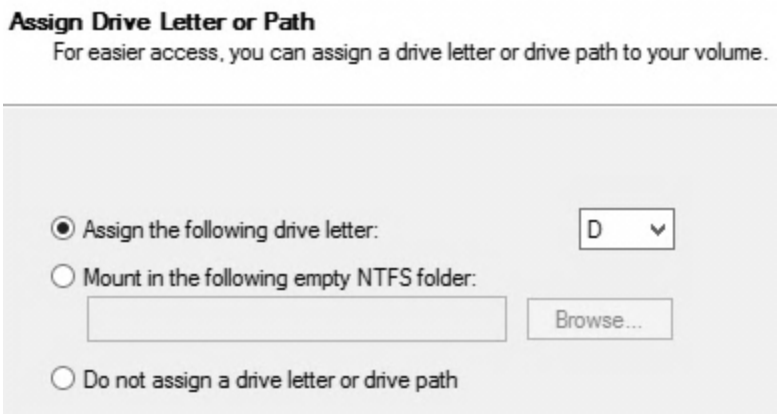
Na podstawie tych danych w razie awarii jednego z dwóch pierwszych dysków można dane odzyskać i serwer będzie dalej działał.



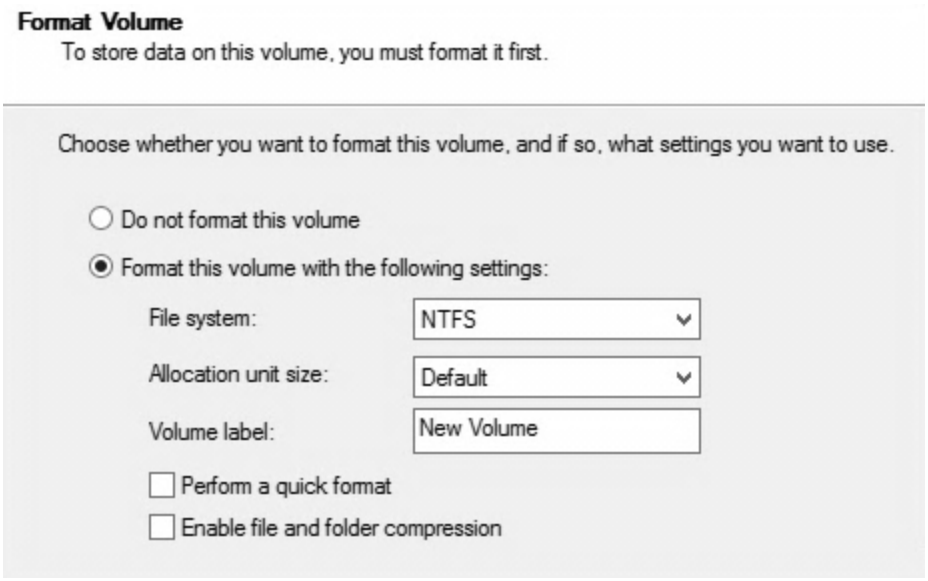
W oknie powitalnym należy kliknąć w Dalej (Next), a następnie wybrać dyski i ustawić odpowiedni rozmiar woluminu. Może on być tak duży, jak duży jest najmniejszy z dysków. Należy kliknąć w przycisk Dalej (Next).



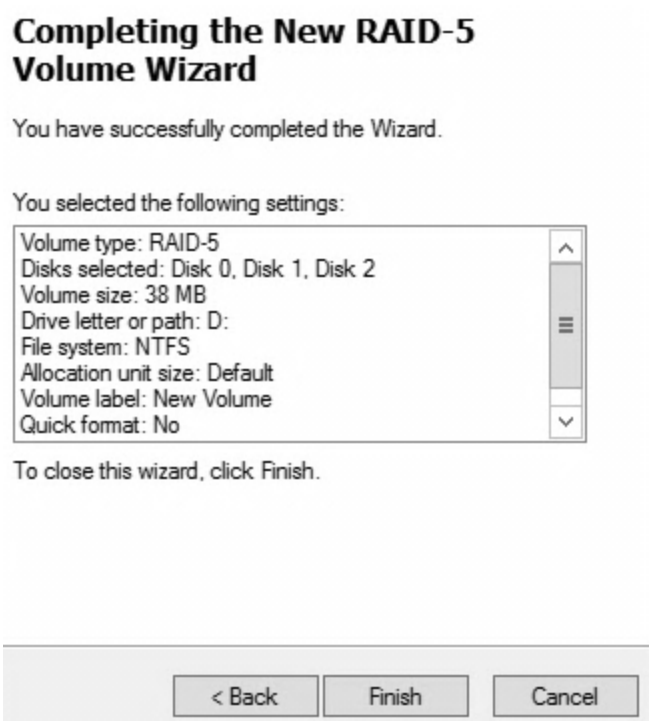
Następnie konieczne jest wybranie litery, która będzie oznaczała dysk.



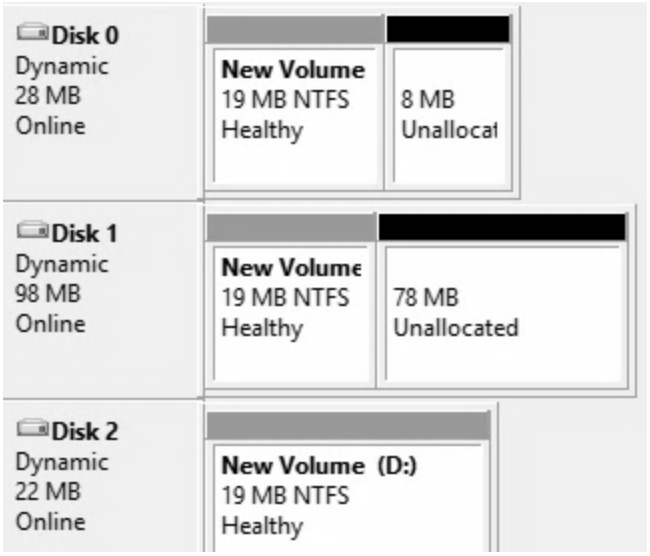
Na kolejne karcie można sformatować wolumin, wybrać odpowiedni system plików, a także nadać mu odpowiednią etykietę. Należy kliknąć Dalej (Next).



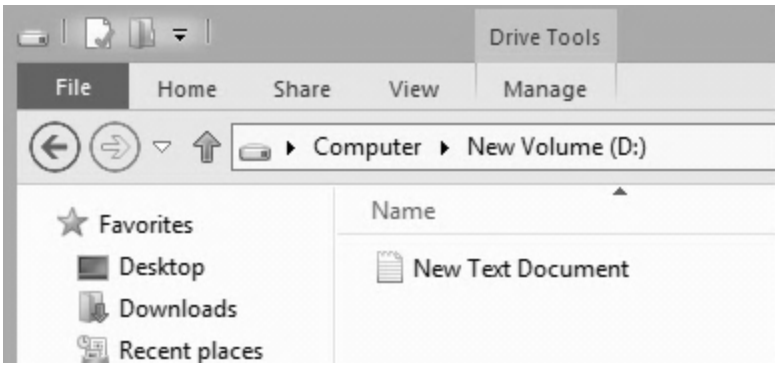
W okienku podsumowującym trzeba kliknąć Zakończ (Finish).



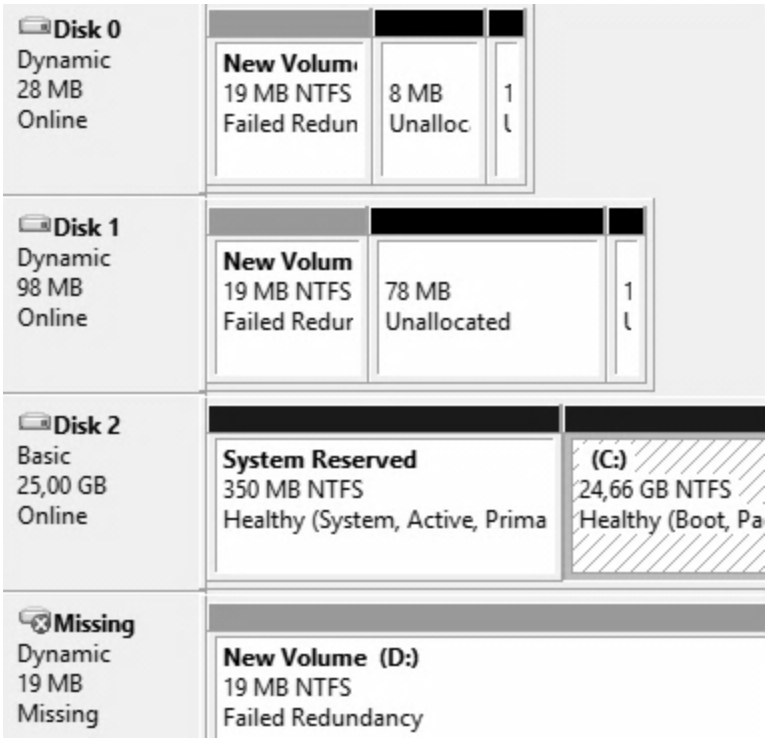
Nastąpi synchronizacja dysków.



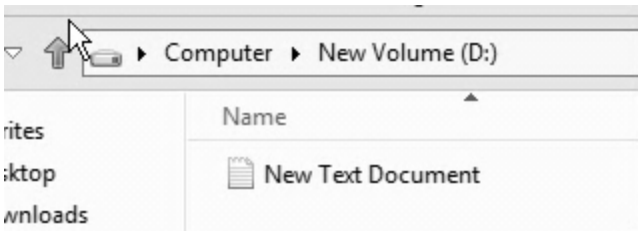
Dla testu zostanie stworzony plik na tym dysku.



W celach testowych maszyna zostanie wyłączona, a jeden dowolny dysk od niej odłączony. Po ponownym uruchomieniu komputera i wejściu do konsoli Computer Management można zobaczyć, że jednego dysku brakuje.



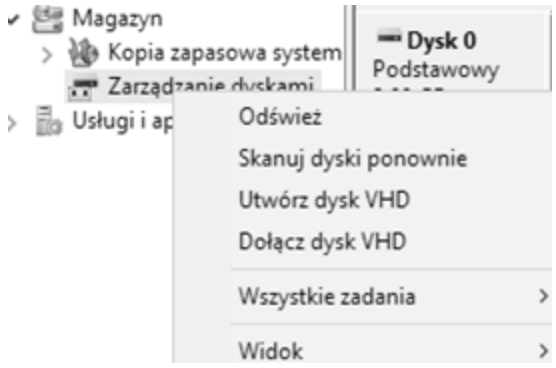
Jednak, jak widać, plik dalej istnieje i ma się dobrze.



13.1. Dyski wirtualne

Dysk wirtualny to określenie zasobów pamięci masowej w komputerze niedostępnych bezpośrednio w systemie, lecz emulowanych przez oprogramowanie w taki sposób, jakby były fizycznie obecne. Najczęściej dysk taki jest realizowany w postaci pliku na fizycznym dysku twardym, który potem jest montowany, dzięki czemu z punktu widzenia użytkownika działa dokładnie tak samo, jak gdyby był to fizyczny dysk twardy.

Po kliknięciu prawym przyciskiem myszy w Disk Management w konsoli Computer Management można w menu kontekstowym ujrzeć dwie opcje związane z tworzeniem wirtualnych dysków: Utwórz (Create) oraz Przyłącz (Attach). Pierwsza z nich służy do tworzenia dysków wirtualnych, druga z kolei do ich podłączania do komputera.



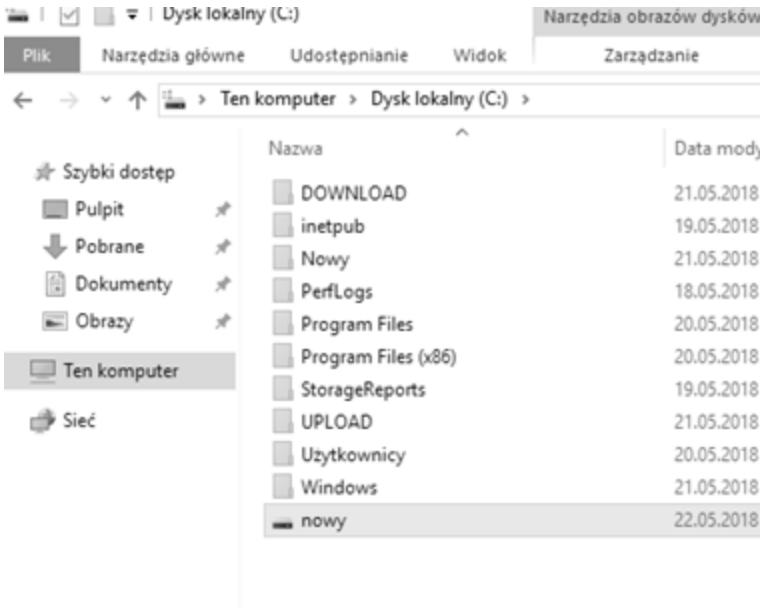
W oknie, które się pojawi, należy podać ścieżkę lokalizacji, w jakiej ma zostać utworzony wirtualny dysk twardy, a także określić jego rozmiar i format. Nowością w systemie Windows Server 2016 jest wprowadzenie

formatu zapisu VHDX, który znosi ograniczenia dysków w formacie VHD. Teraz wirtualny dysk może posiadać objętość do 64 TB, co więcej, VHDX jest bardziej odporny na uszkodzenia, które mogłyby powstać podczas awarii zasilania.

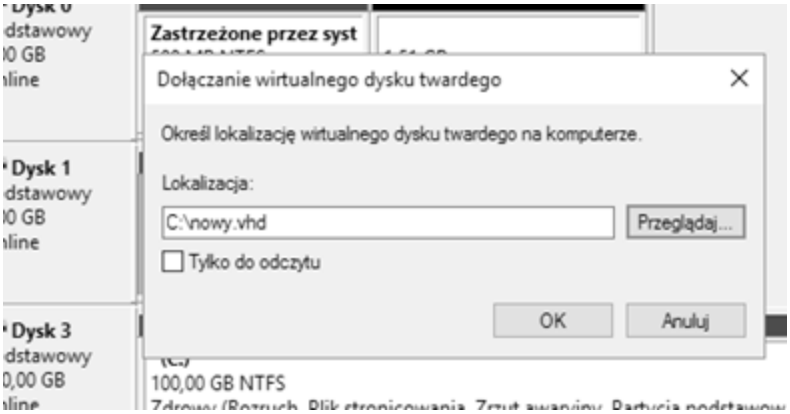
Ostatnim krokiem jest określenie typu dysku wirtualnego. Stały rozmiar (Fixed size) od razu zaalokuje sobie odpowiednią ilość pamięci na dysku fizycznym. Jest rekomendowany ze względu na stabilność oraz szybkość działania. Typ Alokowany Dynamicznie (Dynamically alocated) stworzy dysk, którego rozmiar będzie zwiększany przyrostowo. Im więcej danych zostanie na nim umieszczonych, tym większy będzie rozmiar jego pliku.

Po kliknięciu w przycisk OK i chwili oczekiwania, zależnej od wielkości tworzonego dysku, w podanej lokalizacji

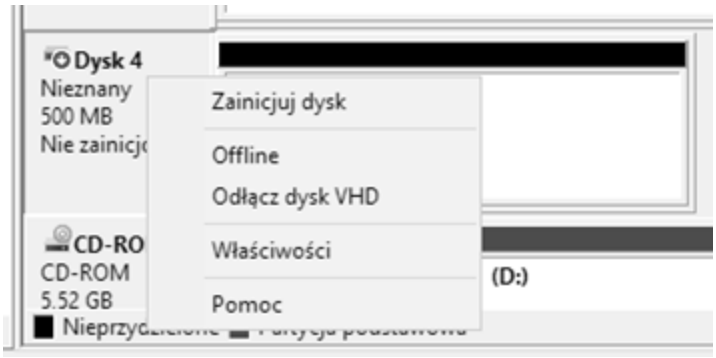
powinien zostać utworzony plik dysku wirtualnego.



Zostanie on także automatycznie podłączony do komputera. Jeżeli jednak wirtualny dysk będzie skopiowany z innej maszyny, należy go podłączyć opcją Przyłącz (Attach) z menu kontekstowego. Wystarczy, że zostanie podana ścieżka i zostanie kliknięty przycisk OK.



Dyskami VHD i VHDX zarządza się tak samo, jak dyskami fizycznymi i również należy je inicjalizować.



Dzięki dyskom wirtualnym można bardzo swobodnie przenosić dane, a nawet całe systemy operacyjne. Co więcej, zwiększają one hermetyczność danych. Wydajnościowo dyski fizyczne i VHD są porównywalne. VHD nieco lepiej wypadają przy zapisie danych.

13.2. Instalacja systemu na wirtualnym dysku

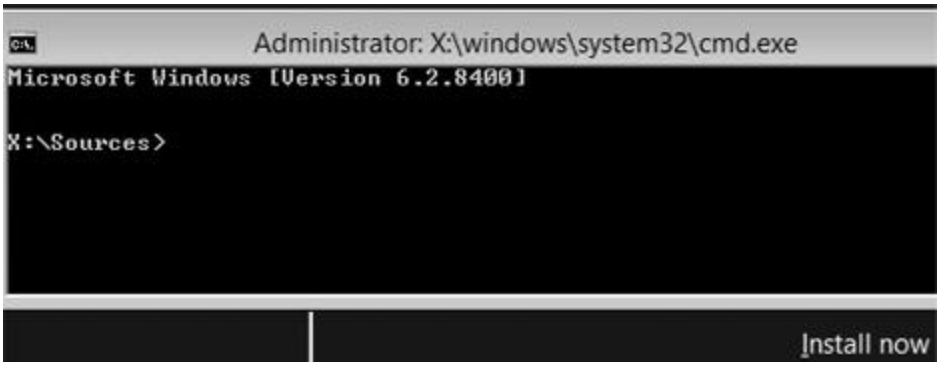
Windows 2016, podobnie jak i Windows 8, Windows 7 czy Windows Server 2008 R2, oferują możliwość instalacji na wirtualnym dysku twardym. Istniała również możliwość takiej instalacji w systemie Windows Vista, lecz nie była ona ani wspierana przez Microsoft, ani w 100% działająca.

Instalacja na dysku wirtualnym polega na tym, że jest on tworzony na istniejącej już partycji z zainstalowanym (choć niekoniecznie, wystarczy, że będzie nim sformatowana partycja) systemem operacyjnym plik VHD. Dzięki temu nie ma konieczności dokupowania dysku ani zmniejszania partycji na obecnym dysku twardym, aby można było zainstalować system operacyjny obok już istniejącego.

Pierwszym pytaniem, jakie powinno się nasunąć, jest celowość takiego zabiegu oraz to, czy jest i jaki jest spadek wydajności. Maszyny wirtualne nie oferują pełnej funkcjonalności sytemu, jak na przykład wsparcie 3D, oraz są zdecydowanie wolniejsze niż zwykłe instalacje. W ten sposób można spokojnie przetestować system pod każdym kątem oraz to, jak będzie działał na sprzęcie fizycznym, a nie wirtualnym.

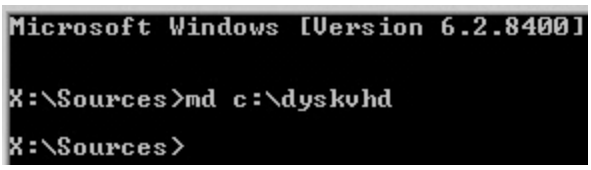
Aby rozpocząć instalację, wystarczy tradycyjnie uruchomić komputer z płyty instalacyjnej Windows 7, a na pierwszym ekranie wybrać odpowiedni język, lokalizację i klawiaturę.

Następnie trzeba wybrać kombinację klawiszy Shift + F10, aby pojawiła się konsola CMD. Instalator to nic innego jak system Windows w wersji PE, czyli polecenia, jak regedit do edycji rejestru itp. zadziałają.

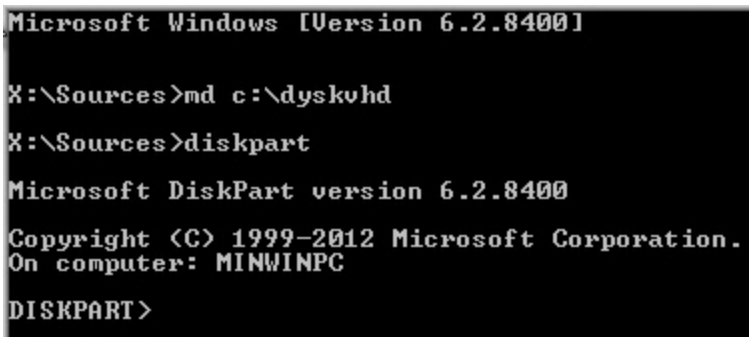


Na komputerze zainstalowany jest już standardowo jeden system. Na dysku 250 GB jest stworzona jedynie jedna

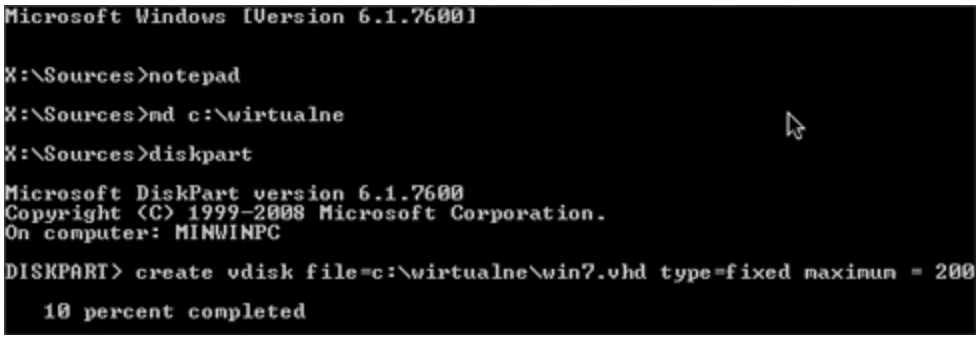
partycja. Na początek warto stworzyć na dysku systemowym C folder, w którym zostaną umieszczone wirtualne dyski.



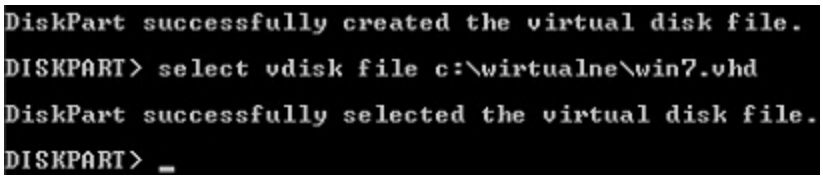
W następnej kolejności należy uruchomić narzędzie do zarządzania dyskami twardymi, wpisując w konsoli polecenie diskpart. Trzeba będzie chwilę poczekać, aż program się załaduje z płyty DVD.



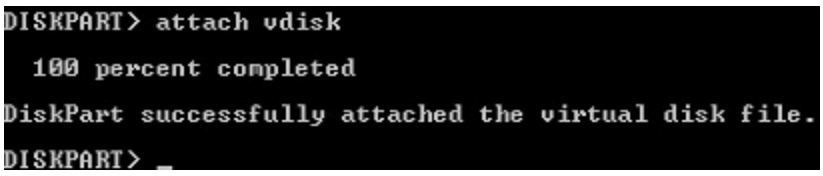
Kiedy program zostanie wczytany do pamięci, należy stworzyć wirtualny dysk twardy. Typ fixed oznacza, że dysk nie będzie dynamicznie się rozszerzał, tylko będzie miał stały rozmiar. Jest to lepsze rozwiązanie, gdyż dyski dynamiczne czasami w tym zastosowaniu powodują pojawianie się niebieskich ekranów. Parametr maximum określa maksymalny rozmiar, jaki dysk będzie miał (przyjmuje on wartości w MB).



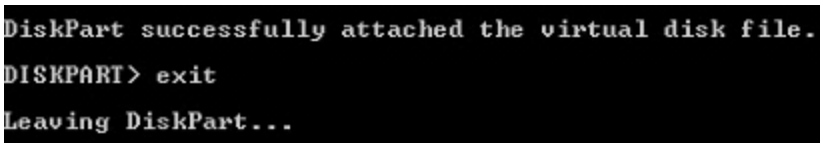
Tworzenie dysku chwilę potrwa, gdyż program w razie potrzeby zdefragmentuje miejsce tak, aby wirtualny nośnik zajmował jedną dużą wolną przestrzeń, która także jest zapisywana zerami przy jej tworzeniu. Gdy dysk zostanie przygotowany, należy go „zaznaczyć”, aby móc na nim operować.



Ostatnim już krokiem będzie przyłączenie dysku poleceniem attach. Jest ono jednoznaczne z fizycznym podłączeniem dysku do komputera.



W dalszym kroku należy zamknąć program poleceniem exit, konsolę krzyżykiem i wrócić do instalatora, klikając Dalej (Next).

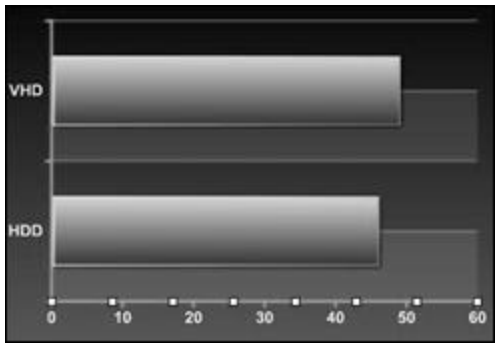


Dalsza instalacja jest analogiczna, jak w przypadku zwykłej instalacji. Wirtualne dyski zostaną automatycznie

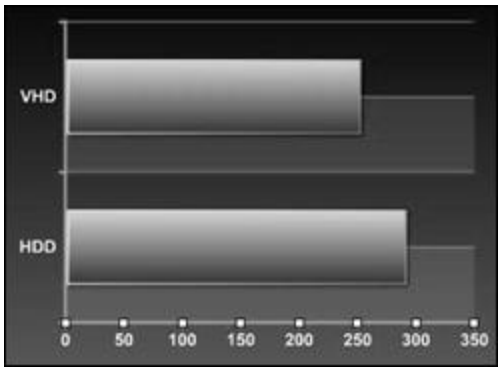
wykryte przez instalator, tak samo jak dyski fizyczne.

Pora przejść do pomiarów wydajności. System działa tak, jakby był normalnie zainstalowany, jedyną różnicą jest to, że mieści się on na sztucznie stworzonym dysku. Dla porównania, poniżej zostały przedstawione wyniki kilku syntetycznych jak i normalnych testów.

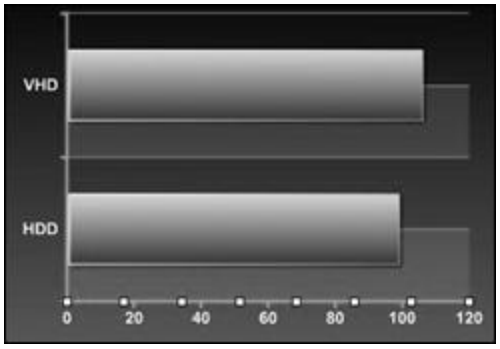
1) Start Windows 7



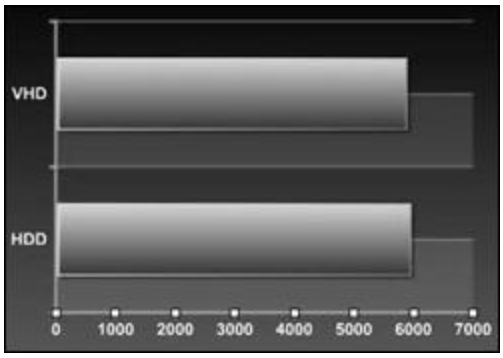
2) Kopiowanie pliku 6 GB



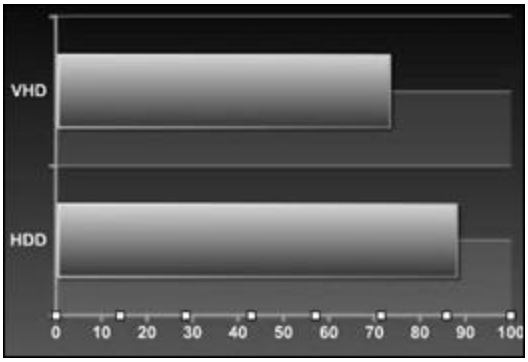
3) Tworzenie pliku 6 GB



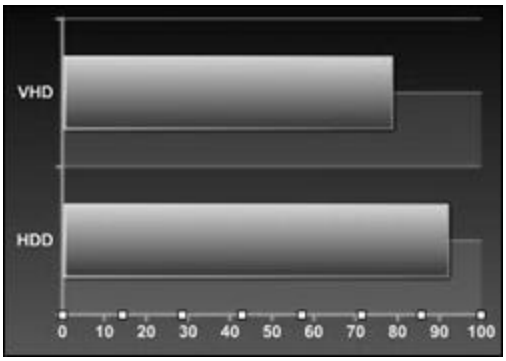
4) PCMark HDD Suite



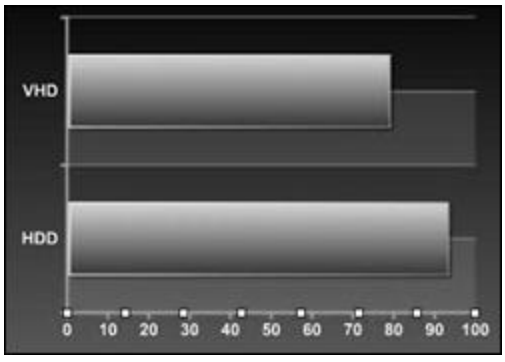
5) HDTune (Mb/s)



6) HDTach 8 MB (MB/s)



7) HdTach 32 MB (MB/s)



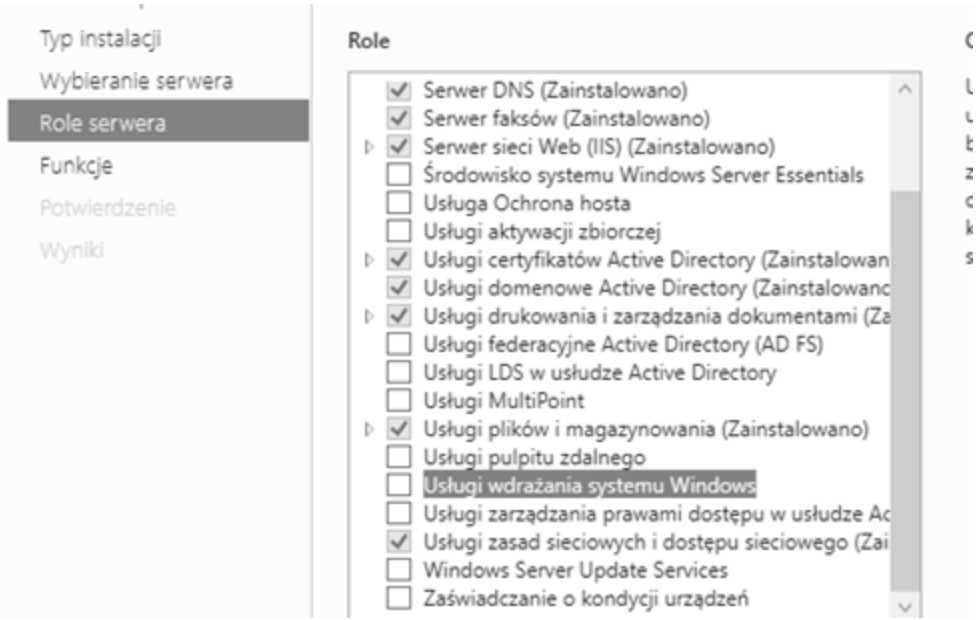
Jak widać, za wyjątkiem kopiowania pliku, dyski VHD są nieco wolniejsze. Nie jest to jednak spadek wydajności na tyle zauważalny, aby się nim bardzo przejmować. Kopiowanie wyszło natomiast nieco lepiej, dlatego że cały obszar pamięci dysku wirtualnego jest zaalokowany jako jeden ciągły obszar. Co za tym idzie, głowica dysku nie musiała daleko się przemieszczać w celu odczytania i ponownego zapisu danych. Wyciągając średnią arytmetyczną z reszty testów, okazuje się, że wydajność dysku wirtualnego jest niższa od zwykłego jedynie o około 10,1%.

Zainteresowanym można także polecić jedną bardzo przydatną aplikację disk2vhd, którą można pobrać ze strony: http://technet.microsoft.com/en-us/sysinternals/ee656415.aspx. Dzięki niej uda się dowolną partycję przekonwertować na dysk VHD. Dla przykładu, jeśli na komputerze jest wgrany Windows XP i użytkownik nie chce go stracić, można wtedy przeprowadzić taką operację. Następnie dysk VHD ze starym systemem można użyć pod Windows 7 do pracy w trybie XP Mode lub jako zwykłą maszynę wirtualną w programie Microsoft Virtual PC.

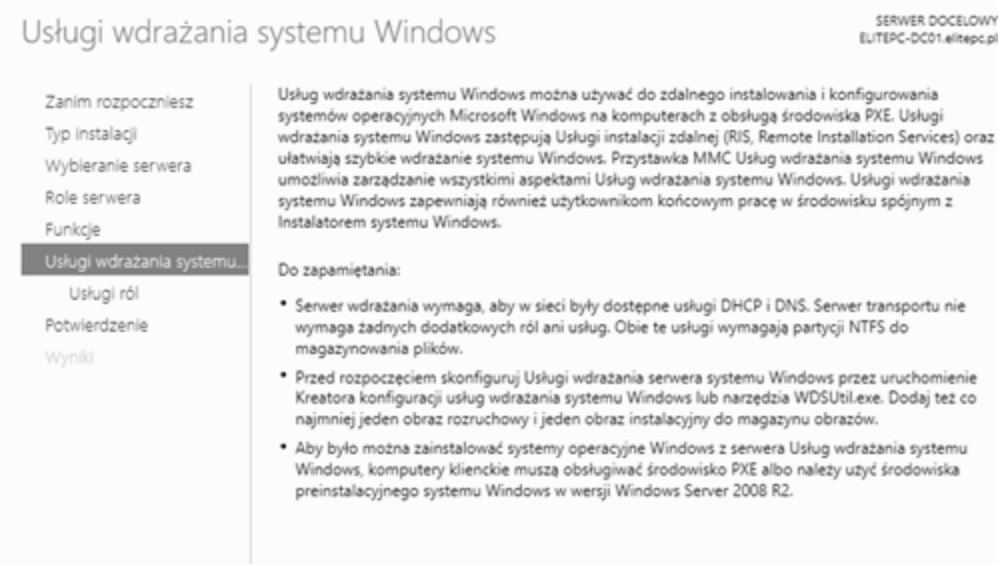
14. WDS – zdalna instalacja

Windows Deployment Services, czyli usługi wdrażania systemu Windows pozwalają na zdalną instalację systemu

na wielu maszynach na raz bez potrzeby używania CD. Komputer dokonuje rozruchu za pomocą połączenia sieciowego, łączy się z serwerem i uruchamia pożądany program instalacyjny, np. Windows Server 2016. Za pomocą aplikacji WAIK można przygotować instalator systemu niewymagający interakcji z użytkownikiem, co znacznie upraszcza wdrożenie oprogramowania na wielu komputerach. W tym celu należy zainstalować rolę systemu Windows o nazwie Usługi wdrażania systemu Windows (Windows Deployment Services). Po wybraniu roli w kreatorze należy kliknąć Dalej (Next).

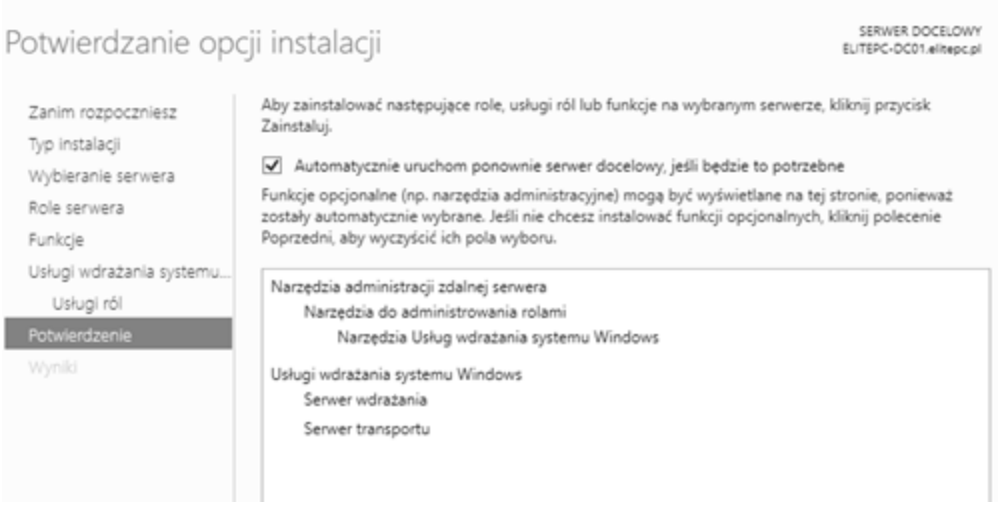


Na kolejnej karcie należy ponownie kliknąć Dalej (Next).

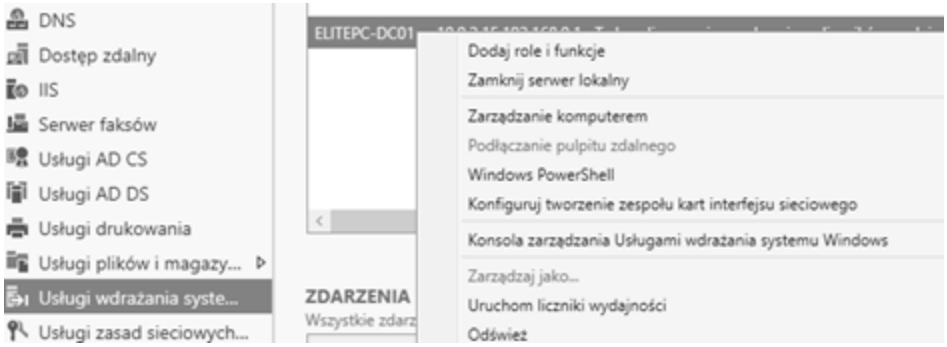


Na następnej karcie należy wybrać odpowiednie Usługi ról (Role Services) i kliknąć w przycisk Dalej (Next).

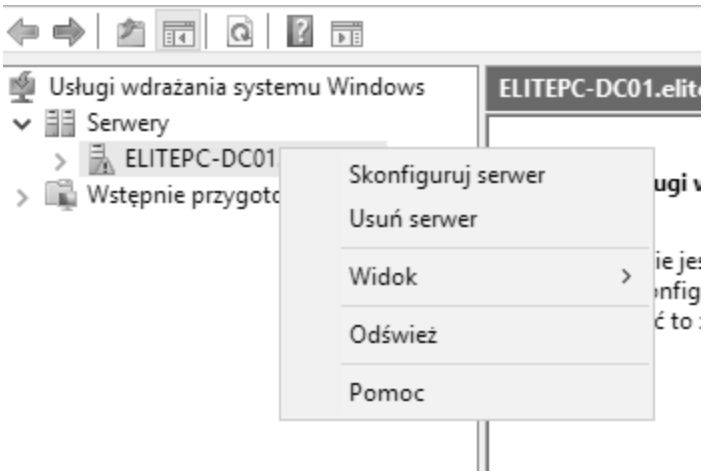
Wybrane wcześniej ustawienia potwierdza się, klikając Instaluj (Install).



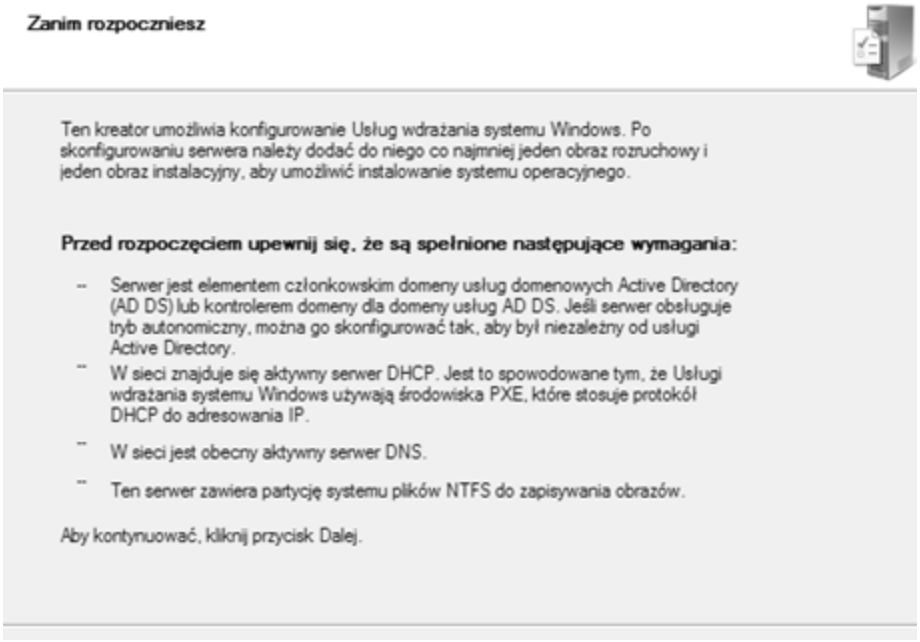
W Menadżerze serwera (Server Manager) pojawi się wpis WDS. Po jego wybraniu i kliknięciu prawym klawiszem w nazwę serwera można na nim uruchomić konsolę Usługa wdrażania systemu Windows (Windows Deployment Services Management Console).



Na serwerze należy kliknąć prawym przyciskiem myszy i wybrać Skonfiguruj serwer (Configure Server).

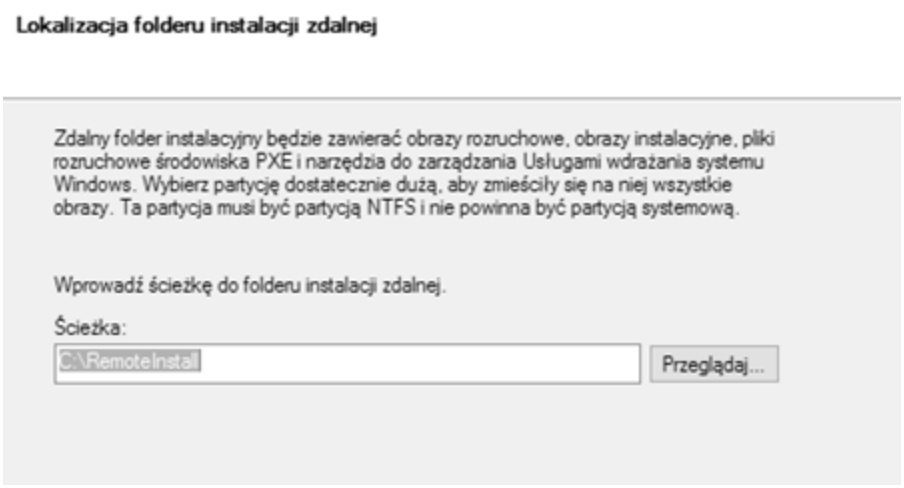


W następnym należy wybrać folder, w którym obrazy systemów mają być przechowywane, i kliknąć Dalej (Next).

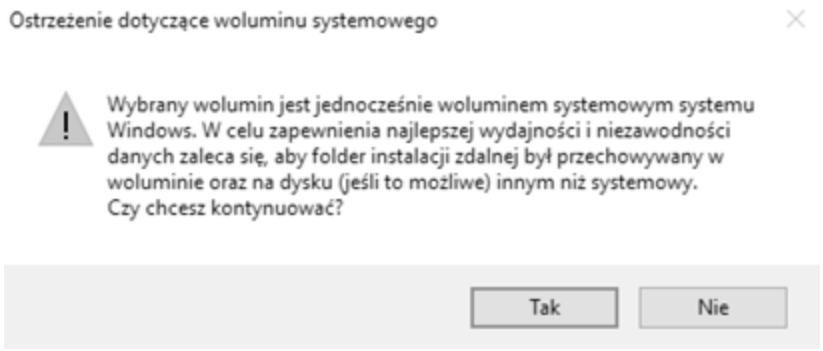


W kolejnym oknie trzeba zdefiniować to, czy serwer będzie działał niezależnie, czy w ramach usługi Active Directory.

Na kolejnym należy wybrać folder, w którym obrazy systemów mają być przechowywane i kliknąć Dalej (Next).

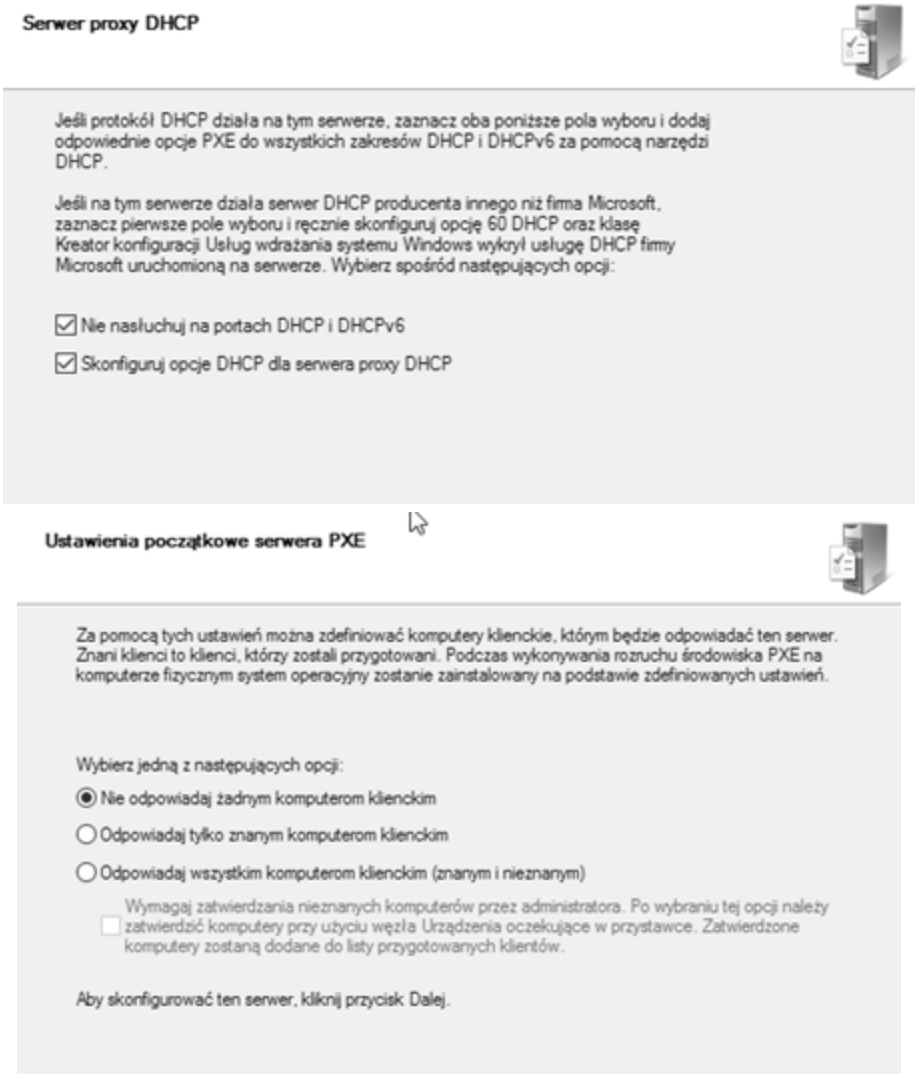


Na komunikacie, który się pojawi, należy kliknąć Tak (Yes).

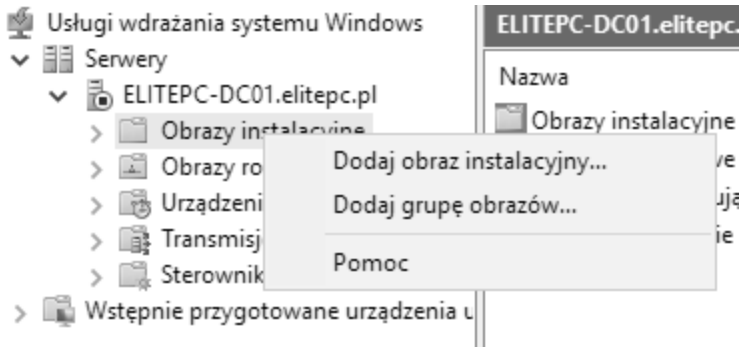


W następnej kolejności wymagane jest zaznaczenie opcji niezbędnych do odpowiadania wszystkim komputerom oraz

kliknięcie Zakończ (Finish).

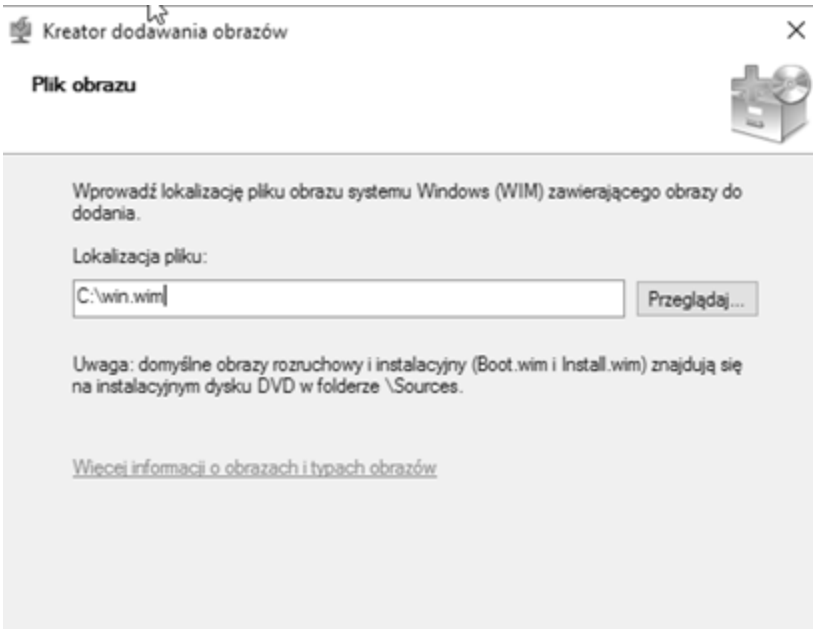


Po kliknięciu prawym przyciskiem myszy w Install Images w konsoli WDS do wyboru będą dwie opcje: Dodaj obraz instalacji (Add Install Image) oraz Dodaj grupę obrazów (Add Image Group).

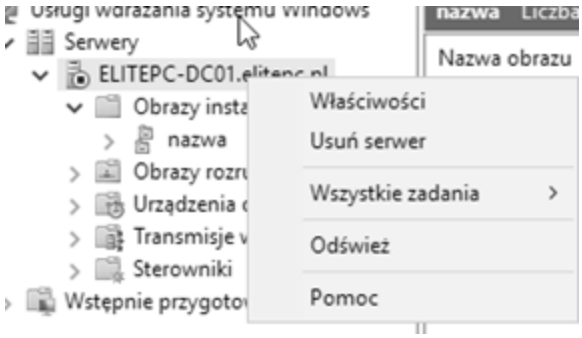


Jeżeli zostanie wybrana ta druga opcja, konieczne będzie podanie nazwy dla grupy.

Teraz niezbędne jest wybranie ścieżki do obrazu lub obrazów systemu. Nie chodzi tu o plik ISO, lecz folder, do którego np. zostanie przekopiowana zawartość instalacyjnego CD. Należy go przygotować narzędziem WAIK.

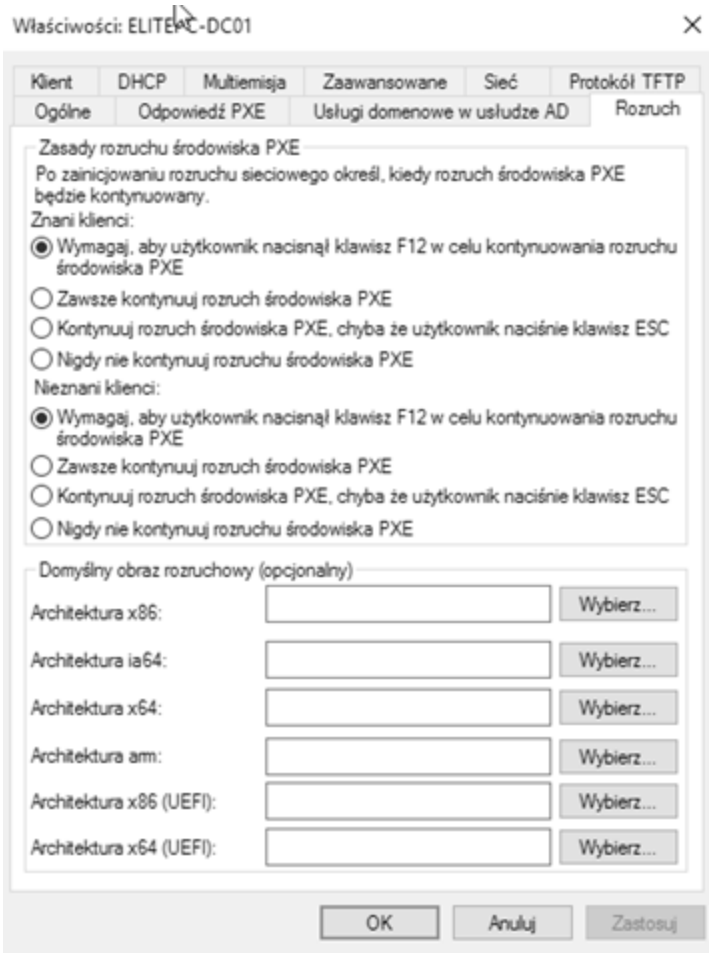


Serwer jest gotowy, by dało się z niego uruchamiać instalację za pośrednictwem sieci lokalnej. Można też przygotować system Windows w wersji PE czy Linux w wersji Live CD.

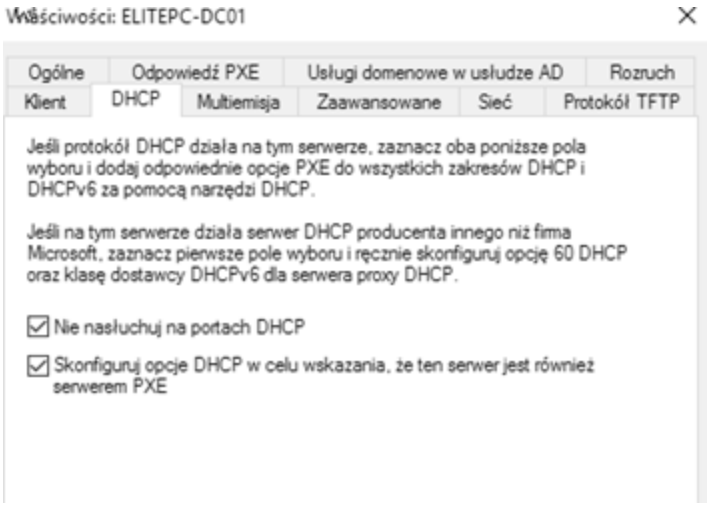


Gdy serwer jest już skonfigurowany przez kreatory, można zawsze dokonać ręcznych zmian jego konfiguracji. Po wejściu we właściwości serwera z poziomu konsoli WDS i wybraniu zakładki Boot można określić parametry związane z rozruchem przez sieć. Definiuje się je osobno dla znanych i nieznanych komputerów klienckich. Między innymi definiuje się to, czy uruchamianie ma być automatyczne, czy na żądanie poprzez wciśnięcie klawisza F12, a także czy

użytkownik będzie mógł przyciskiem Esc anulować proces uruchamiania z sieci. Można także określić domyślne obrazy rozruchowe w zależności od architektury sprzętowej komputera.



W zakładce DHCP należy zaznaczyć obie dostępne opcje, jeżeli każdy komputer, któremu zostanie przypisany adres IP, ma jednocześnie znać adres serwera PXE. Jeśli w sieci jest DHCP pod kontrolą Windows Server, zostanie on automatycznie skonfigurowany, w przeciwnym razie odpowiednie opcje zakresu należy ustawić ręcznie.



Warto także zapoznać się z zakładką Client, gdzie można określić czy każda maszyna, czy tylko ta o określonej architekturze sprzętowej może korzystać z danego obrazu nienadzorowanej instalacji. Nowością w Windows Server 2016 jest wsparcie dla komputerów, które zamiast Biosu używają UEFI. Można tutaj także zabronić podłączania komputera do domeny w sposób automatyczny po instalacji oraz uruchomić logowanie.

15. Hyper – V

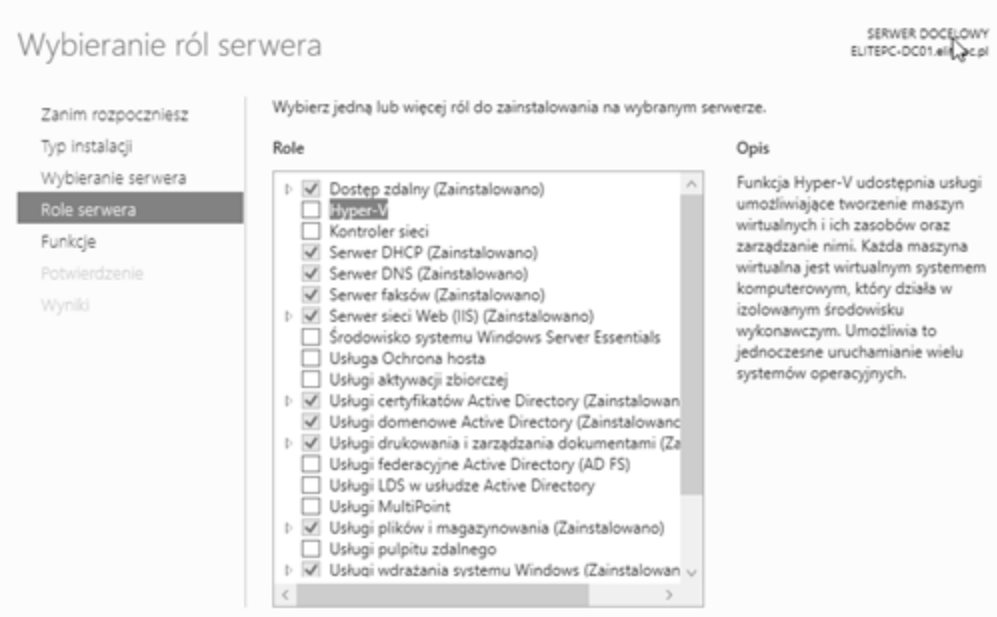
Ostatnie lata rozwoju branży IT naznaczone są słowem wirtualizacja, na której to zaczyna opierać się coraz więcej rozwiązań branżowych. Polega ona na tym, że na fizycznie działającym systemie operacyjnym za pomocą odpowiedniego oprogramowania, w tym przypadku Hyper-V, instaluje się dodatkowy system operacyjny, który zachowuje

się dokładnie tak samo, jak gdyby był zainstalowany na zwyczajnym komputerze.

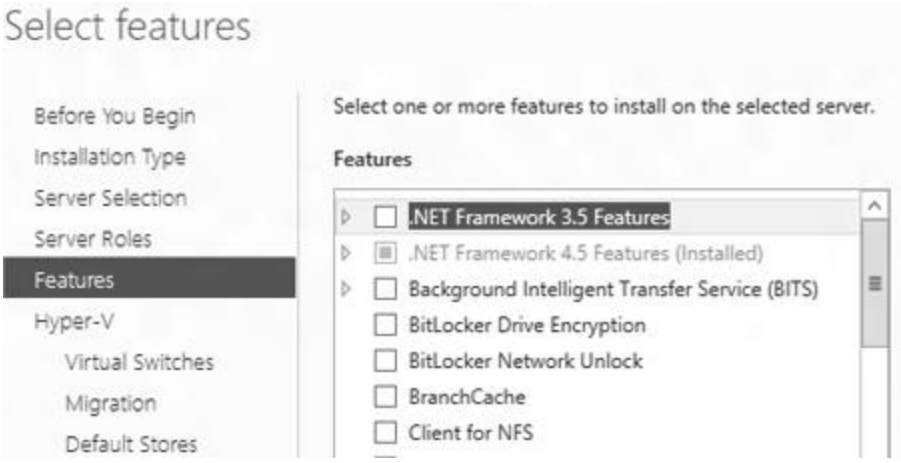
Hyper-V został wprowadzony w Windows Server 2008, został on także rozwinięty o wiele znaczących funkcjonalności w Service Pack 1 do Windows Server 2008 R2. Windows Server 2016 udoskonala istniejące już funkcjonalności, a także wprowadza nowe. W Windows Server 2016 możliwe jest utrzymanie 1024 aktywnych maszyn wirtualnych zamiast wcześniejszych 384. Maksymalną ilość wirtualnych procesorów dostępnych dla maszyny wirtualnej zwiększono z 4 do 32. Pojedyncza maszyna wirtualna może korzystać z maksymalnie 512 GB pamięci (wcześniej 64 GB), a sama rola Hyper-V bez problemu zagospodaruje moc 160 procesorów logicznych.

15.1. Instalacja

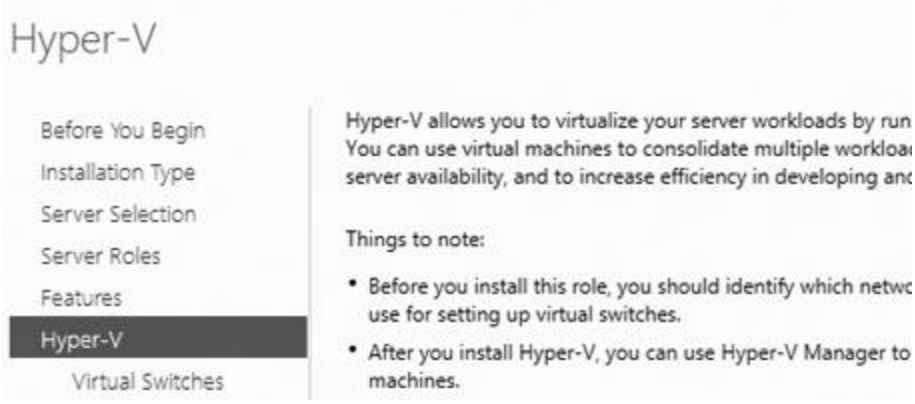
W celu zainstalowania roli Hyper-V należy użyć Menadżera Serwera (Server Manager), w którym podczas dodawania nowych ról wybiera się Hyper-V.



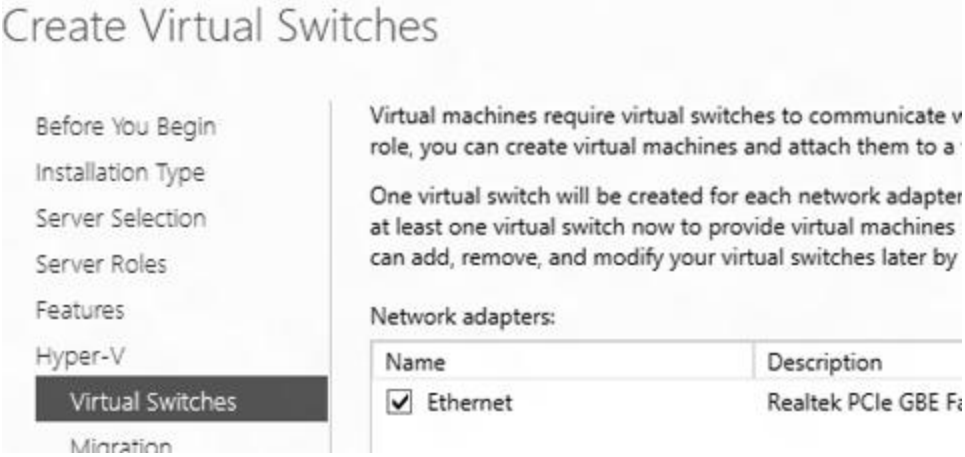
Żadne dodatkowe funkcje nie będą wymagane, więc w oknie ich wyboru można kliknąć w przycisk Dalej (Next).



Kolejne okno kreatora to karta informacyjna, która powiadamia o tym, iż potrzebna jest wiedza na temat tego, które interfejsy sieciowe będą współdzielone z maszynami wirtualnymi oraz, że do zarządzania maszynami wirtualnymi będzie używana konsola Hyper-V Manager. Naturalnie, jeżeli maszyny wirtualne mają mieć dostęp do sieci firmowej, muszą być połączone z interfejsem sieciowym, który jest wpięty do tej sieci.

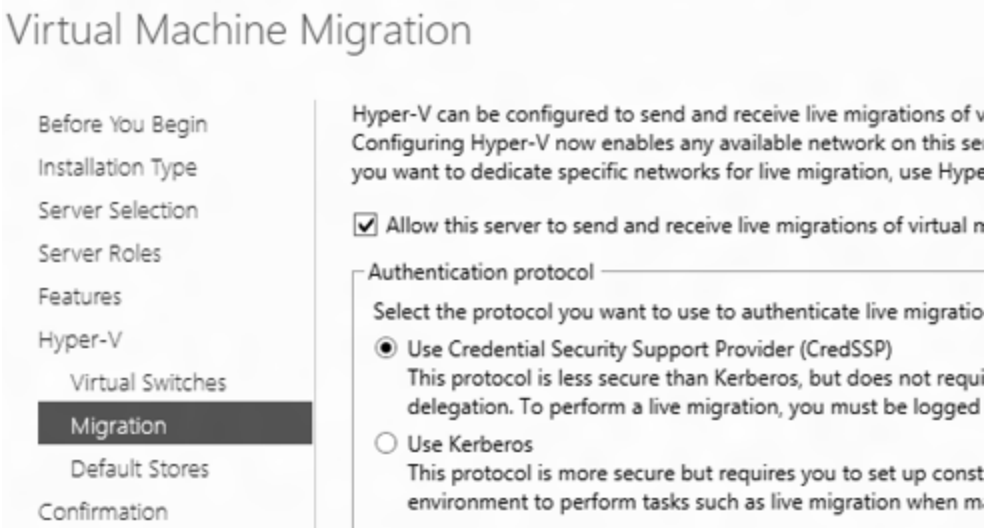


W kolejnym oknie zaznacza się adaptery sieciowe, które mają być użyte. Microsoft rekomenduje pozostawienie jednego interfejsu nieużywanego na potrzeby zdalnej administracji.

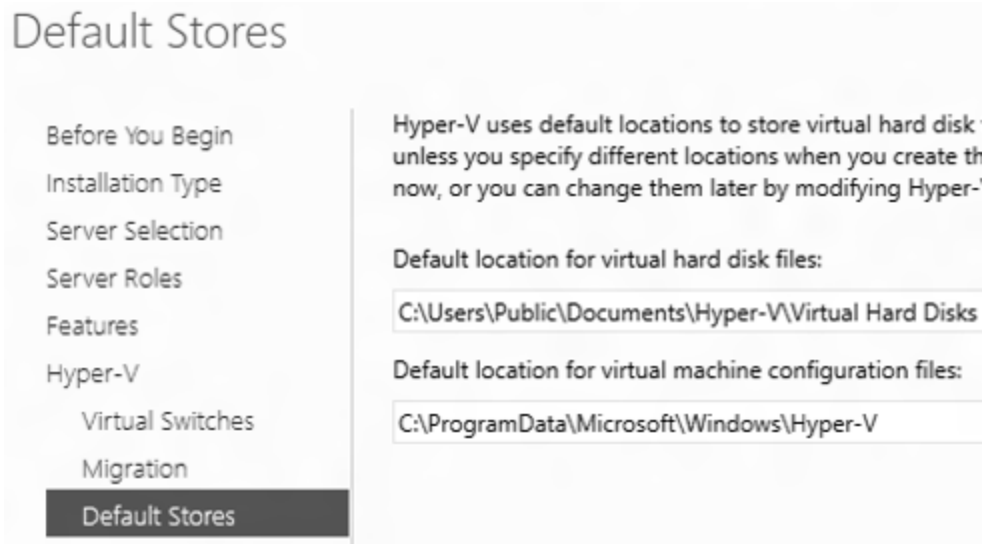


Następna karta kreatora dotyczy ustawień związanych z migracją maszyn wirtualnych. Jest to nowość w systemie Windows Server 2016. Do tej pory niezbędne było używanie funkcji Failover clustering. Do wyboru są teraz dwa rodzaje autentykacji podczas migracji. Jeden z nich to CredSSP, który jest mniej bezpieczny niż protokół Kerberos, lecz nie wymaga tworzenia delegacji, a do przeprowadzenia migracji administrator musi być zalogowany na serwerze źródłowym. W przypadku Kerberosa autentykacja jest bezpieczniejsza, a choć wymaga stworzenia delegacji, pozwala za to na

zdalne wykonanie migracji. Jeżeli serwer ma być częścią klastra, nie należy uruchamiać migracji, lecz zrobić to podczas tworzenia klastra.

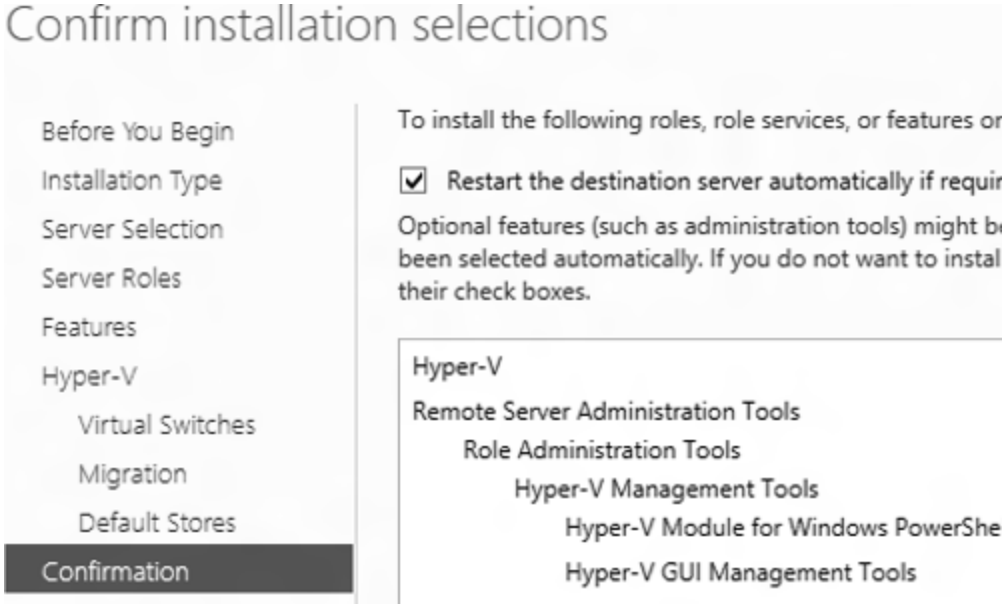


W kolejnym oknie kreatora definiuje się to, gdzie serwer maszyn wirtualnych ma przechowywać wirtualne dyski twarde oraz pliki konfiguracyjne tychże maszyn. Zaleca się trzymać je na szybkich macierzach dyskowych zabezpieczonych przed utratą danych.



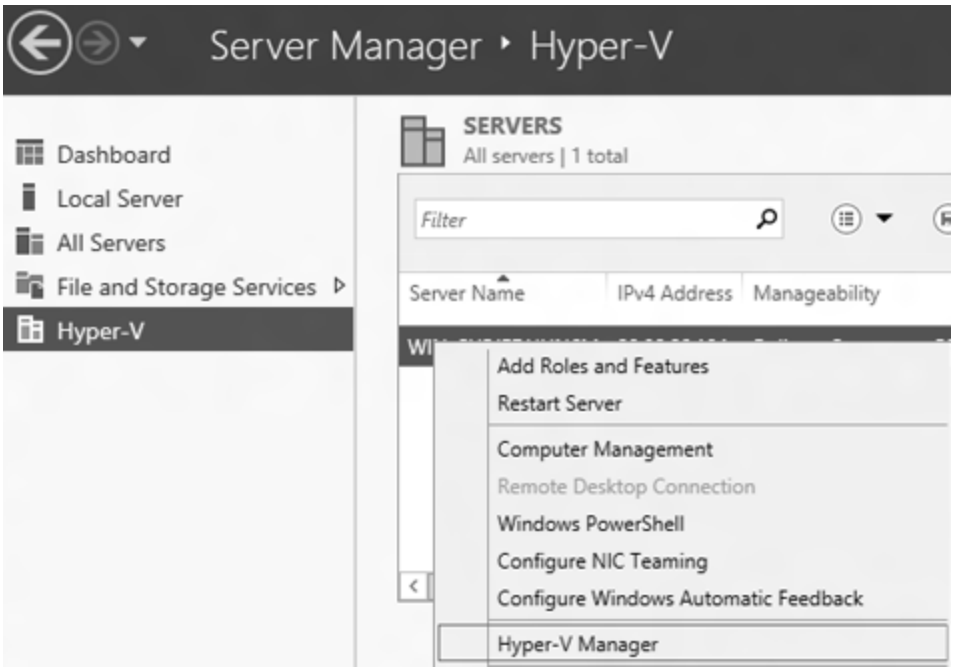
Na karcie podsumowującej należy kliknąć w przycisk Install, aby instalacja się rozpoczęła. Wymagane będzie

ponowne uruchomienie komputera. Na serwerze, na którym zainstalowano Hyper-V, nie zaleca się instalowania innych ról.



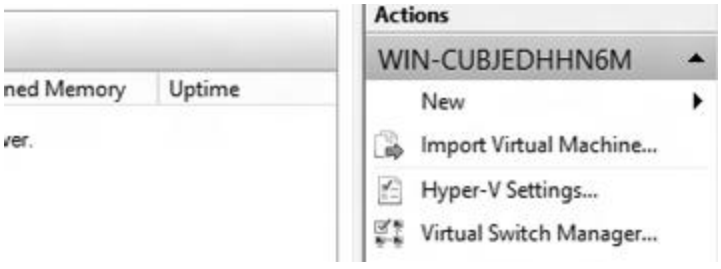
15.2. Zarządzanie Hyper-V

Z poziomu Menadżera Serwera należy wejść do konsoli Hyper-V Manager. Jest to główna konsola zarządzania rolą Hyper-V, w której będzie można wykonywać większość zadań administracyjnych z nią związanych.



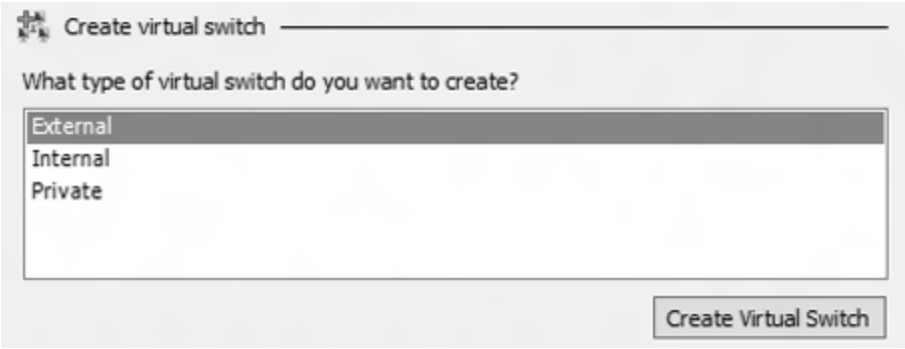
Okno Menadżera Hyper-V składa się z trzech sekcji. Pierwsza z nich to drzewo serwerów pozwalające zarządzać różnymi serwerami, po prawej stronie znajduje się menu, natomiast w centralnej sekcji znajdują się maszyny wirtualne oraz ich migawki. Aby wszystkie funkcje, jak np. zarządzanie RemoteFX i kartami graficznymi, były dostępne, musi zostać zainstalowana także rola Remote Desktop Virtualization, co zostało uczynione w rozdziale 12.

Pierwszym krokiem, jaki powinno się wykonać, jest stworzenie wirtualnych sieci, aby zapewnić łączność ze „światem” dla maszyn wirtualnych. Robi się to przyciskiem Virtual Switch Manager.



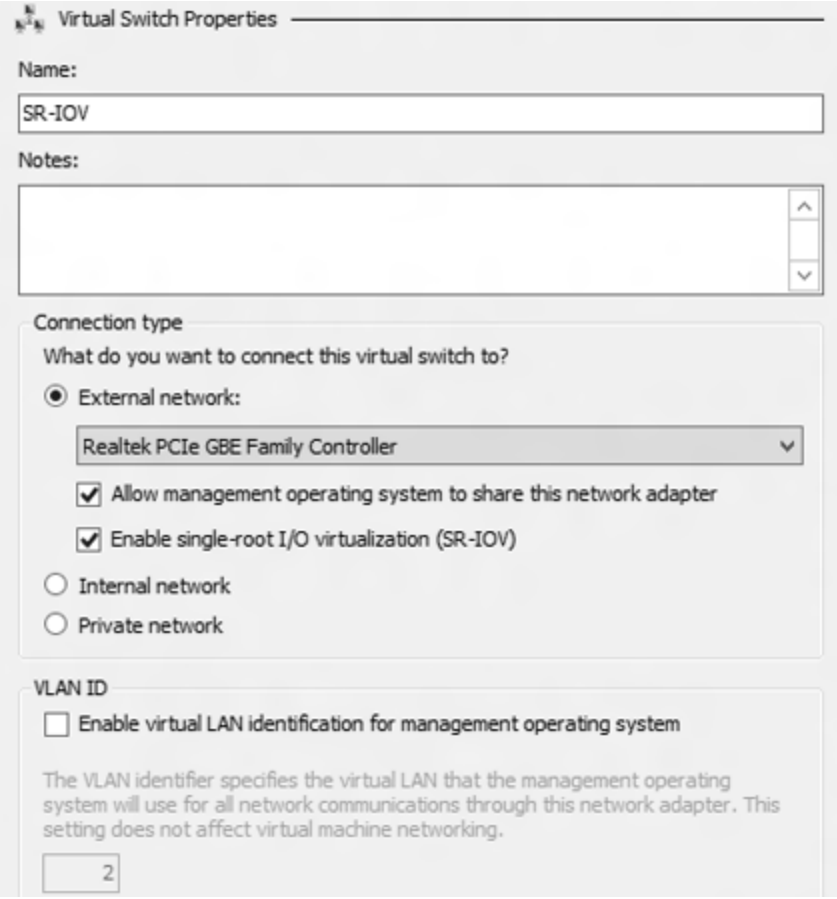
Stworzyć można trzy rodzaje sieci. Jednym z nich jest połączenie zewnętrzne, mostkowane (Bridged), nazwane External. Symuluje ono wpięcie maszyny wirtualnej do fizycznej sieci. Drugim jest połączenie wewnętrzne

(Internal), które tworzy sieć niemającą wyjścia na świat i działającą wyłącznie w obrębie maszyn wirtualnych w taki sposób, że maszyny do niej wpięte będą się między sobą komunikowały. Zapewniona będzie także komunikacja z komputerem hosta (serwerem Hyper-V). Ostatnim rodzajem wirtualnego przełącznika jest sieć prywatna, charakteryzująca się tym, że maszyny wirtualne mają ze sobą łączność. Po wybraniu odpowiedniego wirtualnego przełącznika należy kliknąć Utwórz wirtualny przełącznik (Create Virtual Switch).

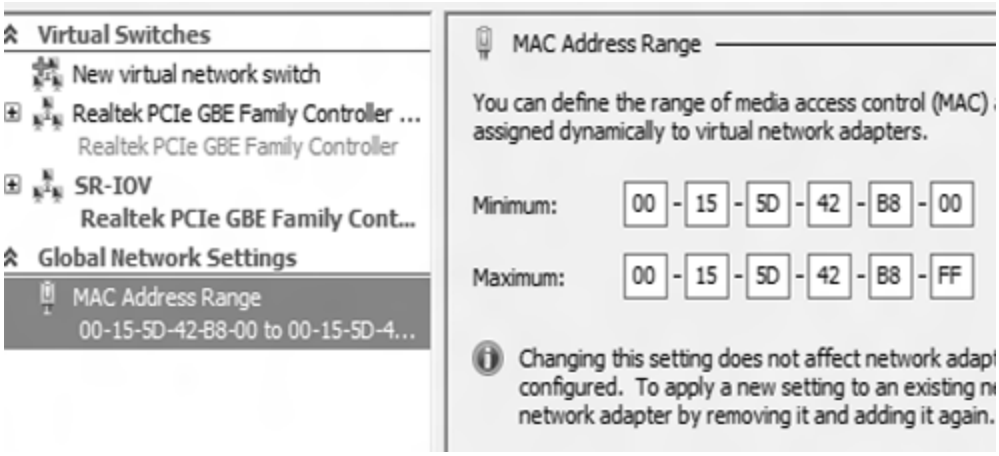


Pojawi się okno, w którym można nadać danemu przełącznikowi nazwę oraz opis; typ połączenia też może zostać zmieniony w każdej chwili. W przypadku połączenia zewnętrznego (External) można z rozwijanej listy określić, do której karty sieciowej połączenie będzie mostkowane. Tylko w tym momencie, czyli podczas tworzenia nowego przełącznika, można skorzystać z funkcji SR-IOV, która jest jedną z nowości w Hyper-V 2016, zaznaczając opcję Enable single – root I/O virtualization. Funkcja ta daje możliwość przypisania karty sieciowej wspierającej standard single root I/O virtualization, co z kolei wpływa na zmaksymalizowanie przepustowości sieci oraz zmniejszenie

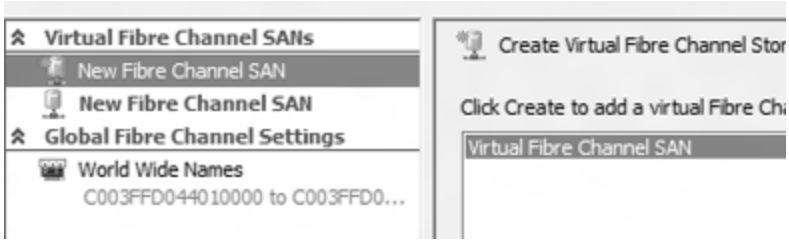
opóźnień sieciowych. Dzięki temu maszyna wirtualna jest bezpośrednio wpięta do fizycznej karty sieciowej bez użycia pośredniczącego wirtualnego przełącznika.



Wybranie w lewym menu **MAC-Address Range** umożliwia zdefiniowanie zakresów adresacji MAC dla wirtualnych kart sieciowych poprzez określenie minimalnych i maksymalnych wartości adresu MAC. Przy użyciu przycisku **OK** należy zapisać i zatwierdzić wybór, jednocześnie zamykając okno i wracając do głównego menu Hyper-V.

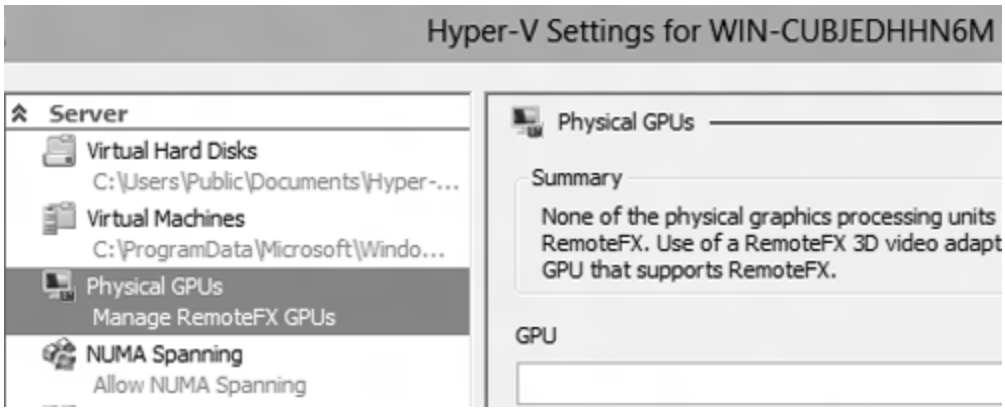


W menu po prawej stronie należy kliknąć w Virtual San Manager, aby zapoznać się z kolejną nowością w Hyper-V. Pozwala ona na stworzenie wirtualnego kanału typu fibre-channel, dzięki któremu maszyny wirtualne mogą mieć dostęp do magazynów typu fibre-channel. Naturalnie wymogiem jest posiadanie portów typu fibre-channel w komputerze hostującym. Należy kliknąć OK.



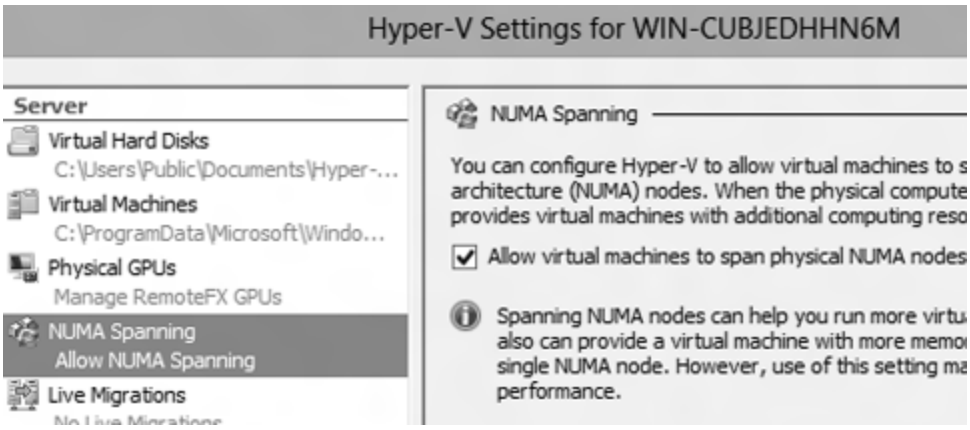
Wracając do Menadżera Hyper-V, można wybrać przycisk Ustawienia Hyper-V (Hyper-V Settings). Pierwsze dwie opcje, czyli Wirtualne dyski twarde (Virtual Hard Disks) oraz Maszyny wirtualne (Virtual Machines), pozwalają na zmianę miejsca przechowywania wirtualnych dysków twardych oraz plików konfiguracyjnych maszyn wirtualnych. Opcja Physical GPUs pozwala na zdefiniowanie, która karta graficzna może być używana przez RemoteFX, a także na włączenie wsparcia GPU dla RemoteFX. RemoteFX jest technologią

wprowadzoną w Service Pack 1 do Windows Server 2008 R2. Daje możliwość wirtualizacji karty graficznej w maszynach wirtualnych, dzięki czemu zyskują one możliwość akceleracji sprzętowej. Pozwala to na renderowanie materiałów 3D, a nawet uruchamianie gier komputerowych. Umożliwia także przekierowanie portów USB do maszyn wirtualnych oraz zapewnia wysoką jakość wideo oraz tekstu.

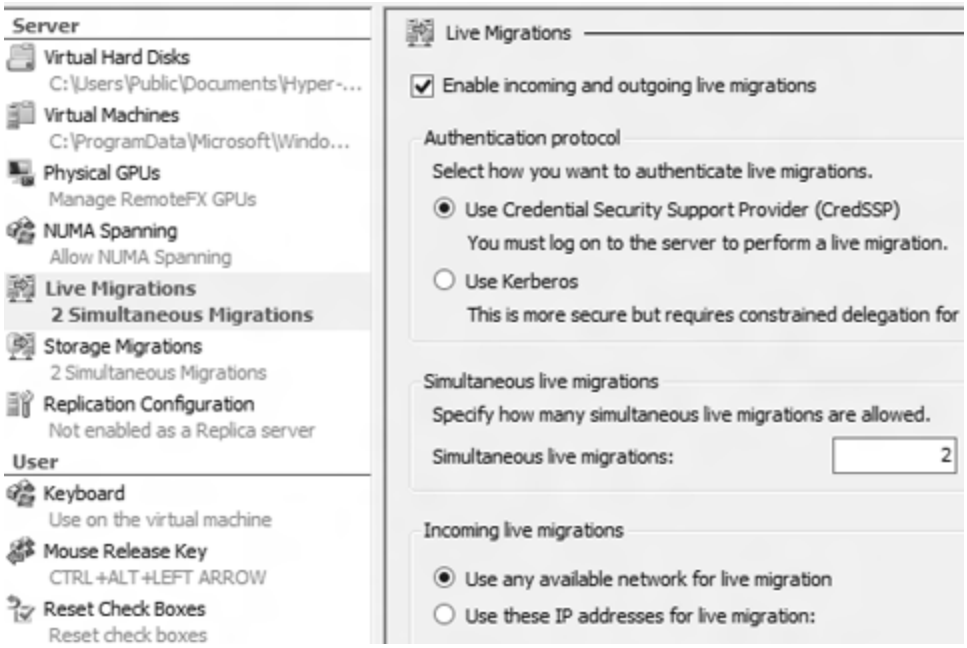


Kolejną opcją wartą omówienia jest NUMA Spanning, którą także można uruchomić w Hyper-V Settings. Technologia ta pozwala na przydzielenie dodatkowych zasobów dla maszyn wirtualnych oraz pomaga w jednoczesnym uruchomieniu wielu maszyn wirtualnych dzięki dynamicznemu przydzielaniu zasobów, jednak w niektórych przypadkach negatywnie wpływa na ogólną wydajność. Jak skorzystać z technologii Virtual NUMA, powiedziane będzie za chwilę przy tworzeniu maszyny wirtualnej. Technologia NUMA nazywana jest także przetwarzaniem współbieżnym nierównomiernym. Stosowana jest ona w szczególności w serwerach wieloprocesorowych, gdzie czas dostępu do pamięci

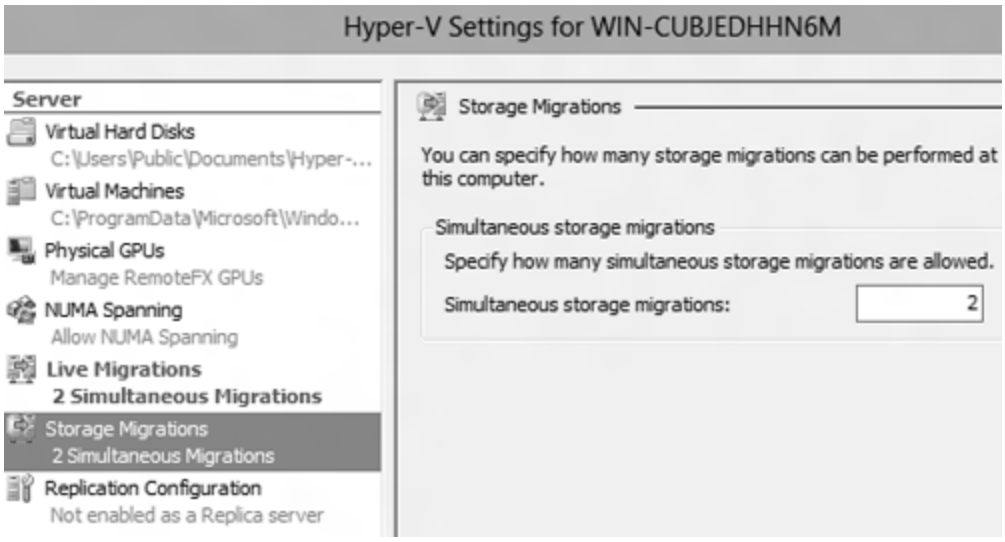
operacyjnej zależny jest od odległości od procesora, który np. szybciej odwoła się do swojej pamięci lokalnej niż do pamięci współdzielonej między procesorami.



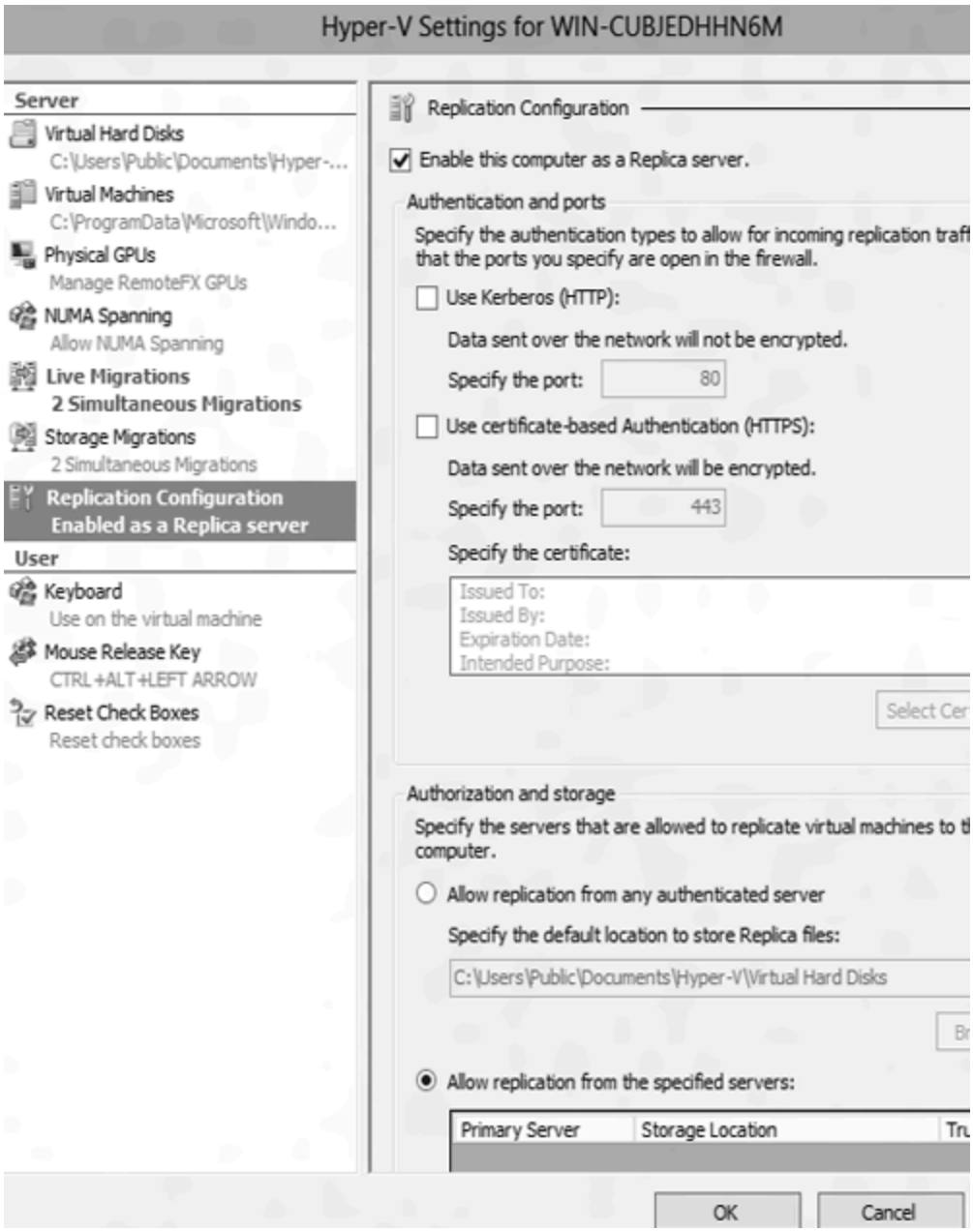
Wybierając opcję Migracja w czasie rzeczywistym (Live Migration) ma się dostęp do opcji, które zostały skonfigurowane w kreatorze instalacji. Można tutaj dodatkowo określić, ile migracji może być jednocześnie przeprowadzanych oraz przez jakie sieci mogą się one odbywać.



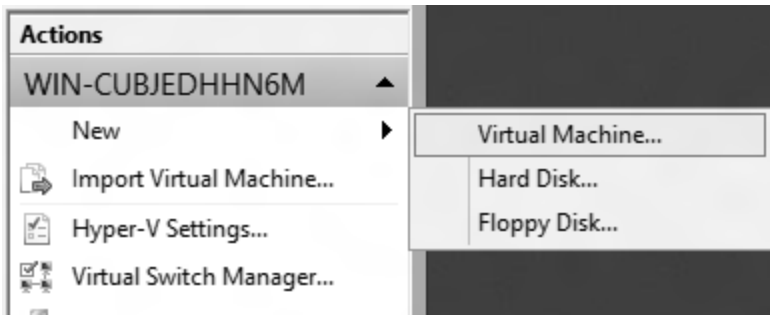
Opcja Migracja magazynów (Storage Migrations) pozwala na określenie, jak wiele migracji magazynów danych może być jednocześnie wykonywane.



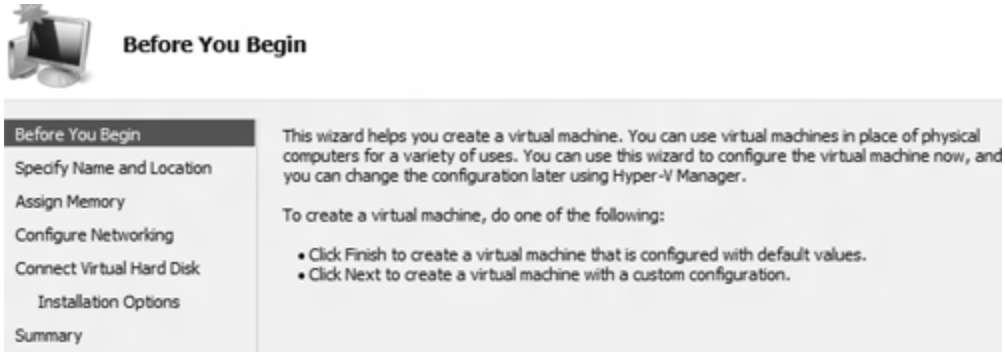
Użycie przycisku Konfiguracja Replikacji (Replication Configuration) pozwala na skonfigurowanie serwera Hyper-V jako serwera przechowującego replikę innych serwerów. Komunikacja pomiędzy serwerami może odbywać w sposób nieszyfrowany, przy użyciu protokołu Kerberos oraz http, lub w sposób szyfrowany, przy użyciu certyfikatów. Jest także możliwość określenia tego, czy mają być przyjmowane repliki z dowolnego serwera, czy z określonej listy, którą można zdefiniować.



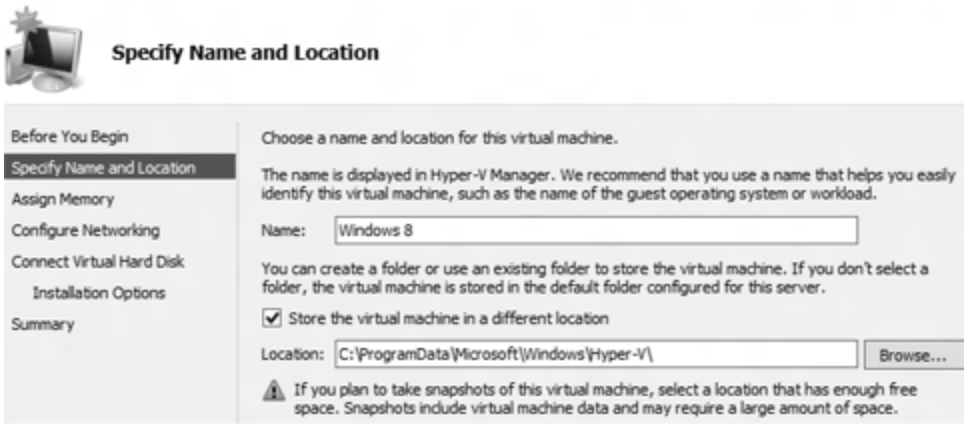
Nową maszynę można stworzyć z poziomu Menadżera Hyper-V, importując ją bądź tworząc nową przy użyciu przycisku Nowy (New), a następnie wybierając Wirtualna maszyna (Virtual Machine). Można stworzyć także obraz dyskietki czy wirtualny dysk twardy.



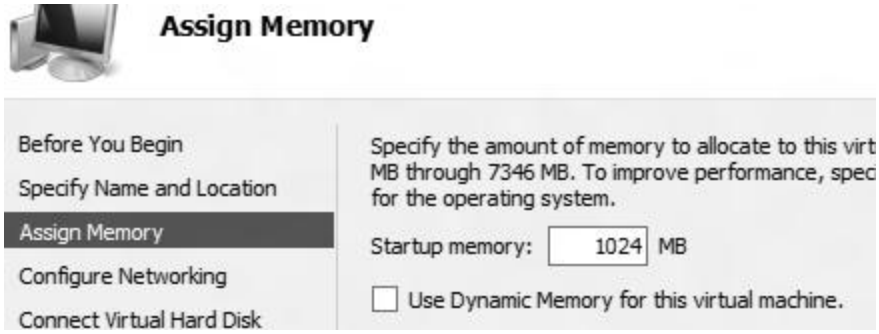
Otworzy się okno kreatora, a kliknięcie w przycisk Zakończ (Finish) spowoduje stworzenie maszyny wirtualnej z predefiniowanymi ustawieniami, stworzonymi przez firmę Microsoft. Jeżeli jednak administrator pragnie mieć większy wpływ na konfigurację wirtualnego komputera, powinien kliknąć w przycisk Dalej (Next).



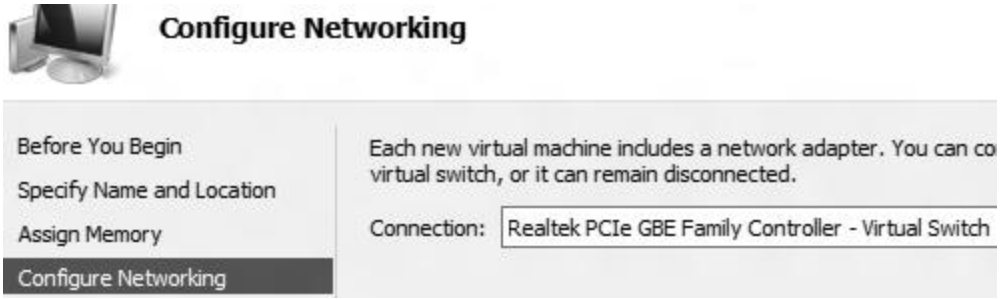
W kolejnym oknie kreatora określa się nazwę maszyny wirtualnej i ewentualną inną lokalizację na dysku twardym. Warto też zauważyć, że w każdej chwili można użyć przycisku Zakończ (Finish), aby zakończyć kreatora pozostawiając pozostałe opcje domyślne. W przypadku książkowym zostanie kliknięty przycisk Dalej (Next).



Na kolejnej karcie określa się, ile pamięci RAM zostanie przydzielone tej maszynie wirtualnej. Można także włączyć dynamiczne alokowanie pamięci, o czym więcej będzie za chwilę.

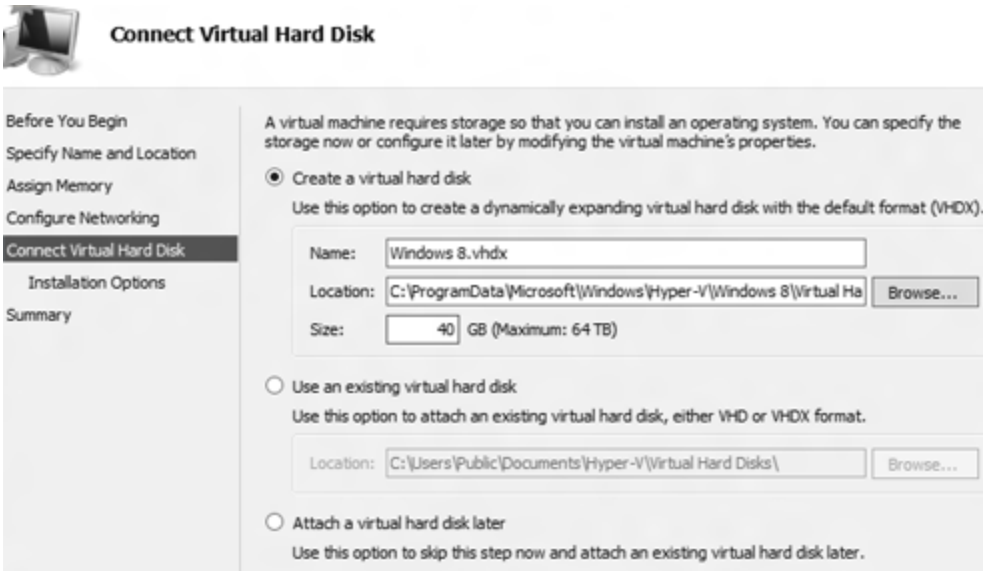


Następnie określa się wirtualny przełącznik, który zapewni komunikację z siecią.

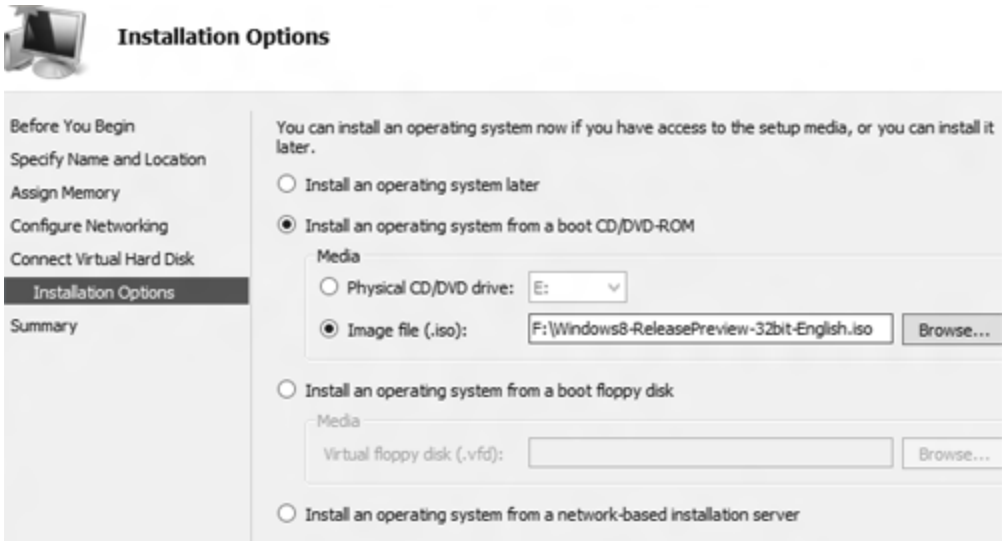


Kolejny krok to tworzenie lub przyłączanie wirtualnego dysku twardego. Są trzy opcje do wyboru. Pierwsza – Utwórz wirtualny dysk twardy (Create a virtual hard disk) to stworzenie dysku twardego w formie pliku. W tym

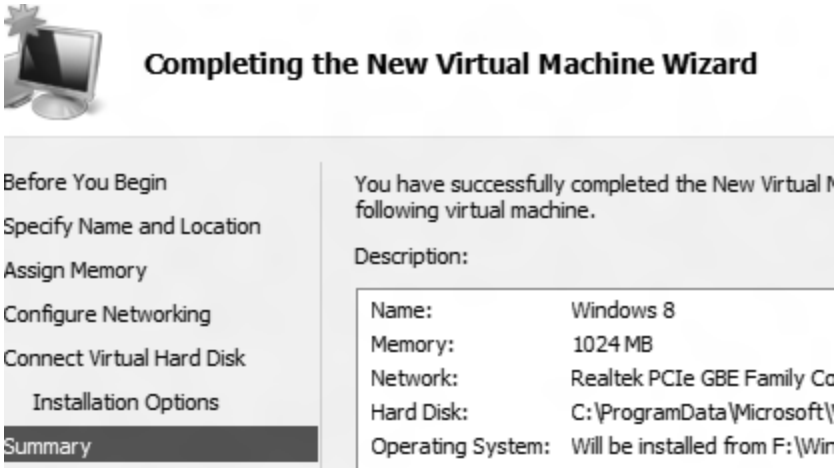
przypadku wystarczy podać jego rozmiar w GB. Druga opcja – Użyj istniejący wirtualny dysk twardy (Use an existing virtual hard disk) to wykorzystanie istniejącego już wirtualnego dysku twardego w formacie VHD lub VHDX. Trzecia – Przyłącz wirtualny dysk twardy później (Attach a virtual hard disk later) to przyłączenie wirtualnego dysku w czasie późniejszym. Jako że nie został wcześniej stworzony żaden dysk twardy – należy stworzyć go teraz.



Następny krok dotyczy instalacji systemu operacyjnego w maszynie wirtualnej. Można albo wykonać to w późniejszym czasie, albo podmontować napęd CD gospodarza zamiennie z obrazem ISO płyty, jak również zainstalować system operacyjny z obrazu dyskietki lub sieciowego serwera rozruchu. W tym przypadku zdecydowano się na instalację systemu Windows Server 2016 z obrazu ISO.

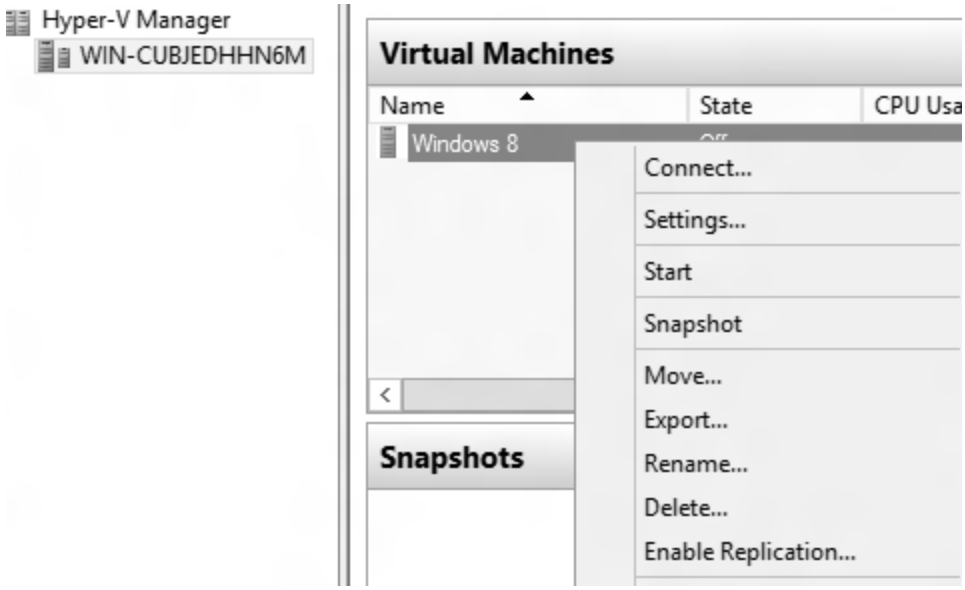


Ostatnim krokiem kreatora będzie wyświetlenie karty podsumowującej, na której należy kliknąć w przycisk Zakończ (Finish).



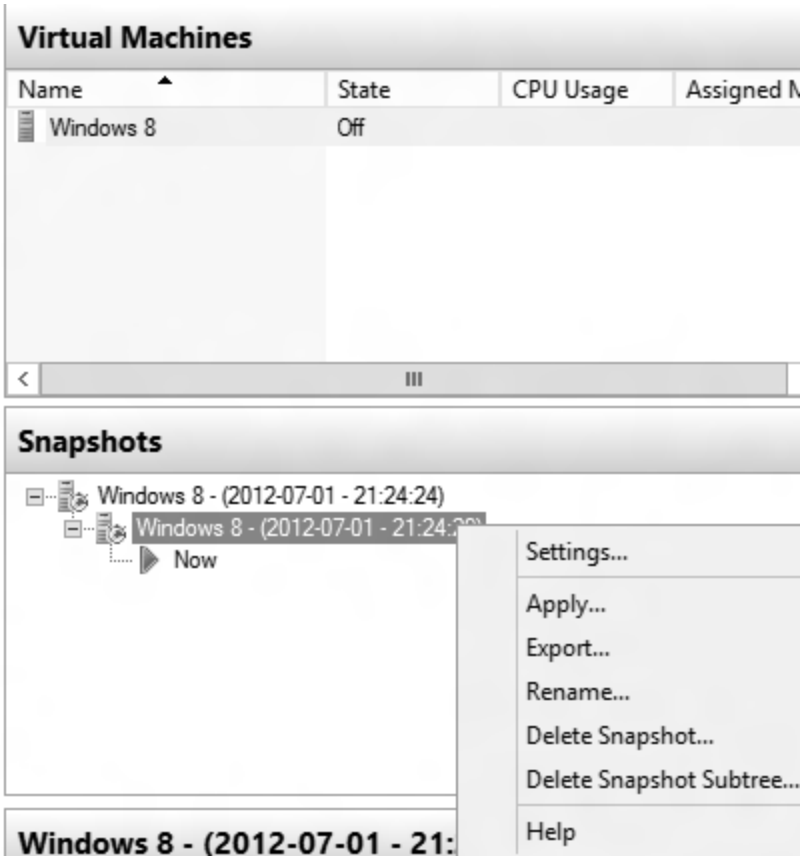
Wirtualna maszyna pojawi się w Menadżerze Hyper-V w sekcji Maszyny Wirtualne (Virtual Machines). W menu kontekstowym myszy bądź po wybraniu maszyny wirtualnej w menu po prawej stronie ekranu wyświetlą się dodatkowe opcje. Pierwszą z nich jest Połącz (Connect), pozwalający na wyświetlenie okna maszyny wirtualnej, które jest realizowane na zasadzie połączenia pulpitu zdalnego. To samo można uzyskać dwukrotnym kliknięciem na maszynie

wirtualnej. Opcja Start (Start) uruchamia maszynę wirtualną. Opcja Przenieś (Move) uruchamia kreator przenoszenia maszyny wirtualnej. Opcja Eksportuj (Export) pozwala na wyeksportowanie maszyny wirtualnej w celu jej zaimportowania na innych komputerach. Opcja Zmień Nazwę (Rename) zmienia nazwę, a opcja Usuń (Delete) usuwa maszynę. Przydatna może się także okazać opcja Włącz Replikację (Enable Replication), która uruchomi kreatora ustawień replikacji dla tej maszyny wirtualnej. W kreatorze między innymi będzie konieczne wskazanie serwera docelowego bądź brokera replikacji w przypadku klastra.



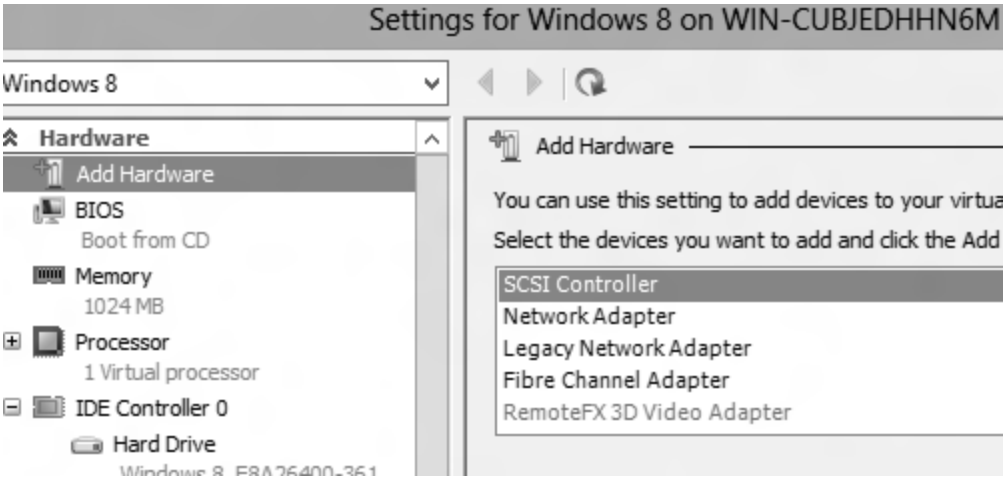
W menu kontekstowym znajduje się także opcja Migawka (Snapshot), która tworzy migawki stanowiące jakby „zamrożone” wersje zainstalowanego systemu. Migawki pojawiają się w sekcji Migawki (Snapshots), a w ich menu kontekstowym można migawkę zastosować przyciskiem Zastosuj (Apply), co spowoduje wyzerowanie stanu

maszyny wirtualnej do stanu z migawki. W menu kontekstowym znajdują się także opcje Eksportuj (Export) do eksportowania migawek i Zmień nazwę (Rename) do zmiany ich nazwy. Jest też możliwość usunięcia samej migawki lub całego drzewa migawek opcją Usuń (Delete).

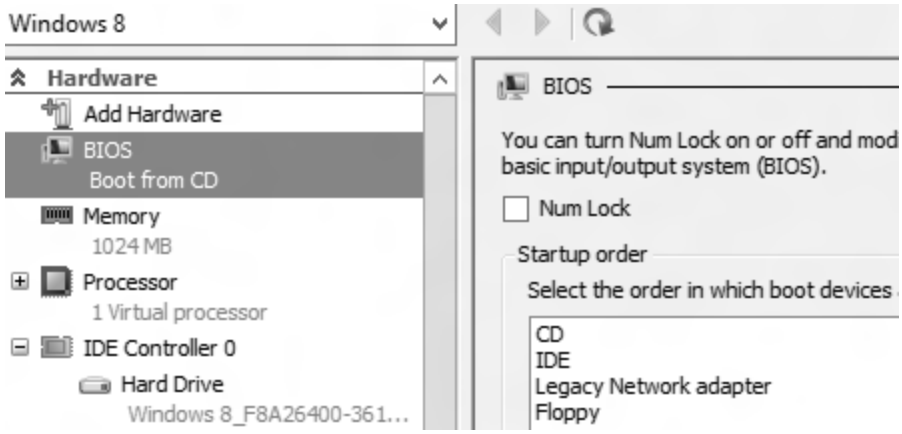


Kliknąwszy na maszynie wirtualnej prawym klawiszem myszki i wybrawszy opcję Ustawienia (Settings), można dostać się do ustawień wirtualnego komputera. Zostanie otwarte okno konfiguracji, a w nim zaznaczona opcja Dodaj sprzęt (Add Hardware), pozwalająca na przypisanie maszynie wirtualnej dodatkowych urządzeń. Są nimi kontroler SCSI, karta sieciowa, stara karta sieciowa, która może być zainstalowana na starych komputerach, adapter

fibre-channel oraz karta graficzna 3D poprzez funkcję RemoteFX.

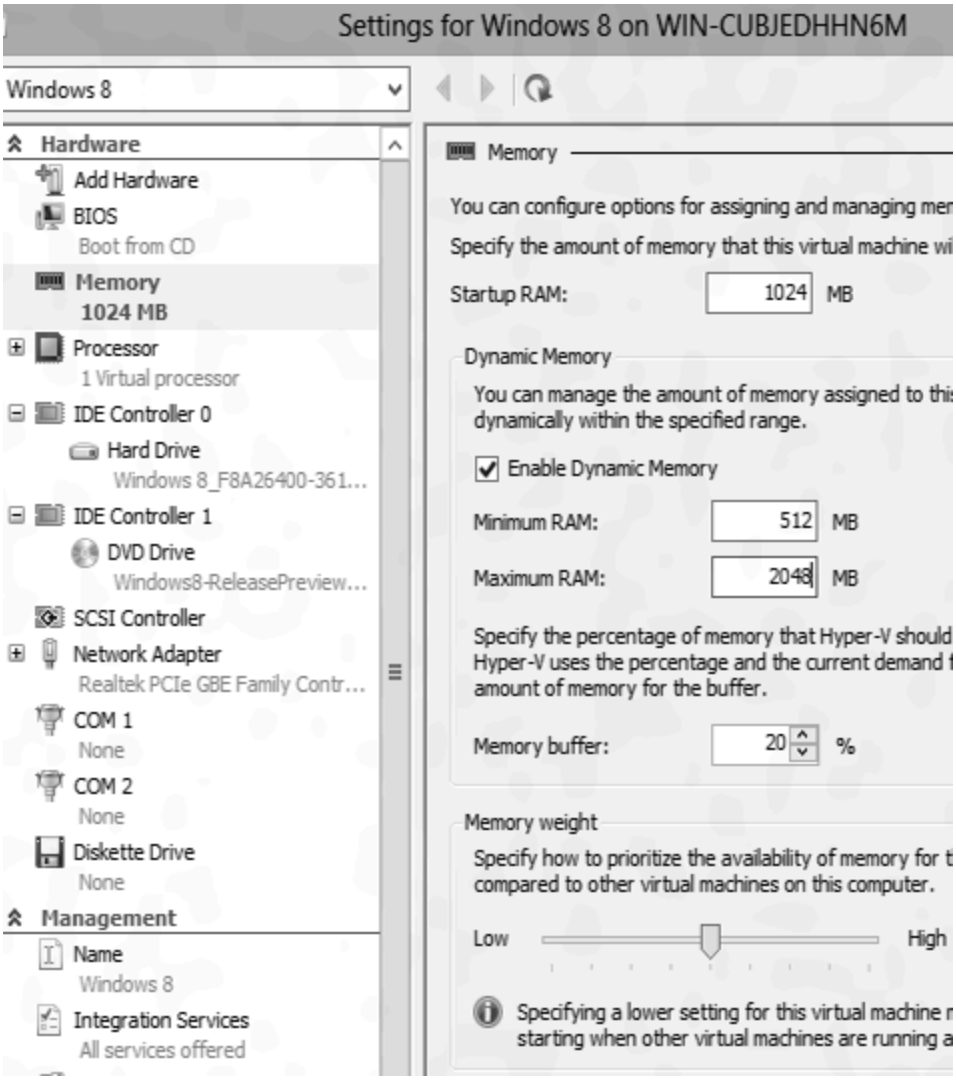


W sekcji Bios definiuje się kolejność urządzeń startowych w komputerze.



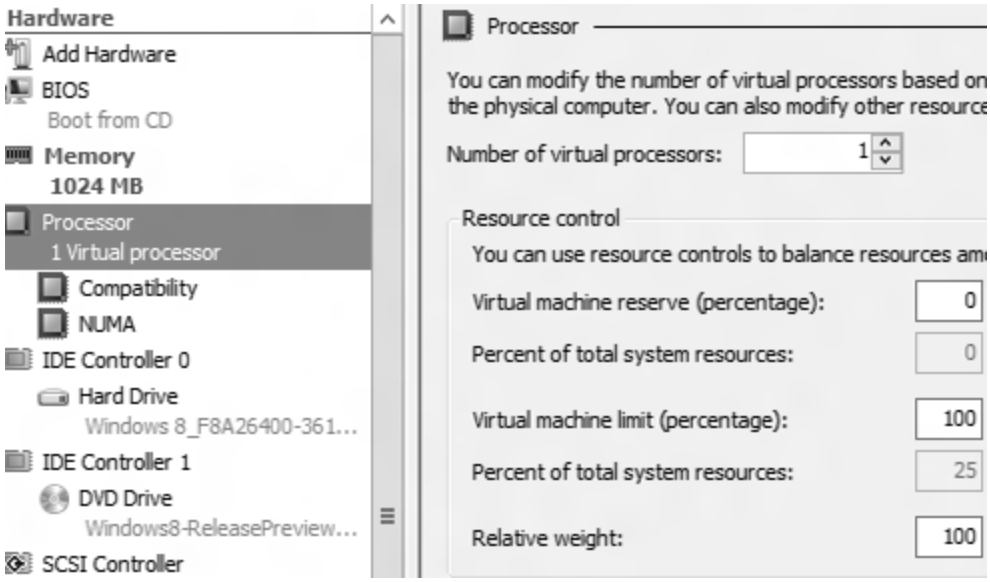
Klikając na odnośnik Pamięć (Memory) można ustawić stałą ilość pamięci RAM przypisaną danej maszynie bądź uruchomić pamięć dynamiczną i określić minimum, jakie maszyna musi mieć przydzielone oraz maksimum, które będzie mogła mieć przydzielone, gdy zajdzie taka potrzeba i obciążenie innych maszyn na to pozwoli. Za pomocą suwaka w sekcji Priorytet Pamięci (Memory Weight) określa się priorytet dla tej maszyny wirtualnej. Maszyna

o najwyższym priorytecie będzie miała przydzielaną pamięć w pierwszej kolejności.

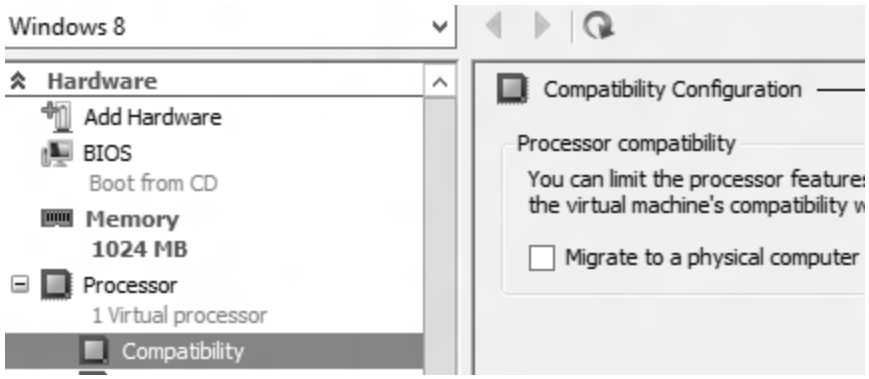


Po kliknięciu w Procesor (Processor) administrator ma możliwość określenia ilości wirtualnych procesorów przydzielonych maszynie, a także ustawienia kontroli zasobów, ponieważ te same procesory prawdopodobnie będą dzielone z innymi maszynami. Między innymi można także określić procentową rezerwację mocy procesora oraz procentowo maksymalne zużycie procesora, jak również

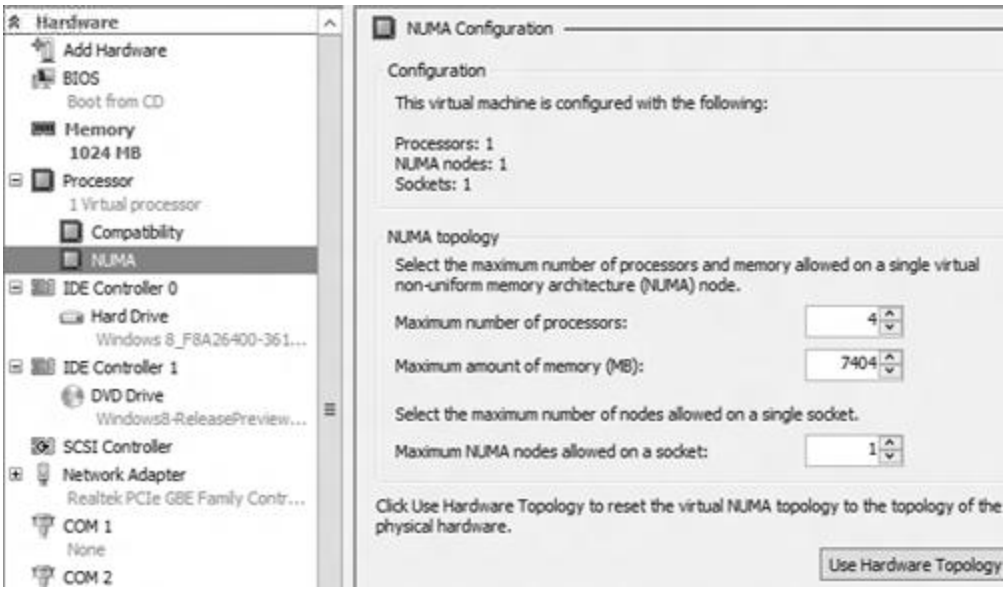
priorytet, który działa analogicznie do pamięci dynamicznej pod parametrem Relatywny Priorytet (Relative Weight).



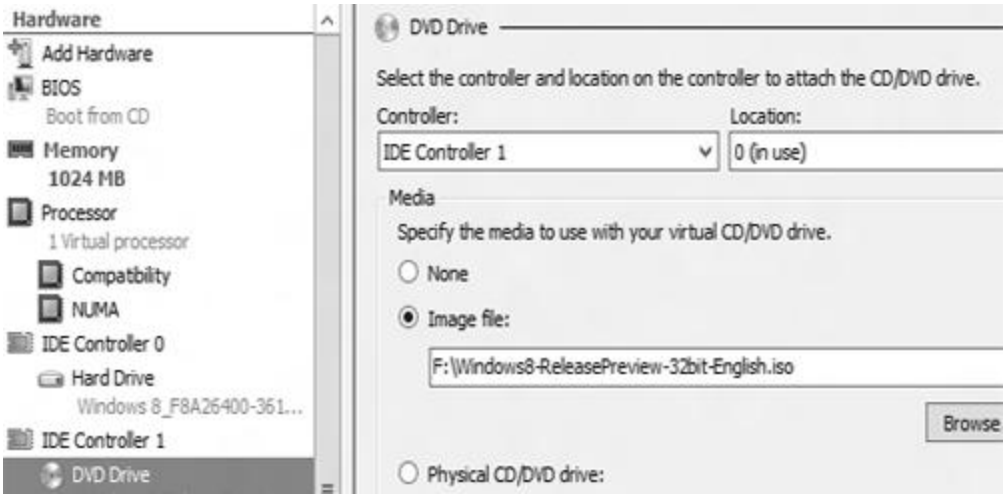
W momencie, gdy zostanie rozwinięte drzewo, procesor i wybrana opcja Kompatybilność (Compatibility), istnieje możliwość wybrania opcji migracji na komputer z innym procesorem. Przydaje się ona wtedy, gdy maszyna została zaimportowana na innym hoście.



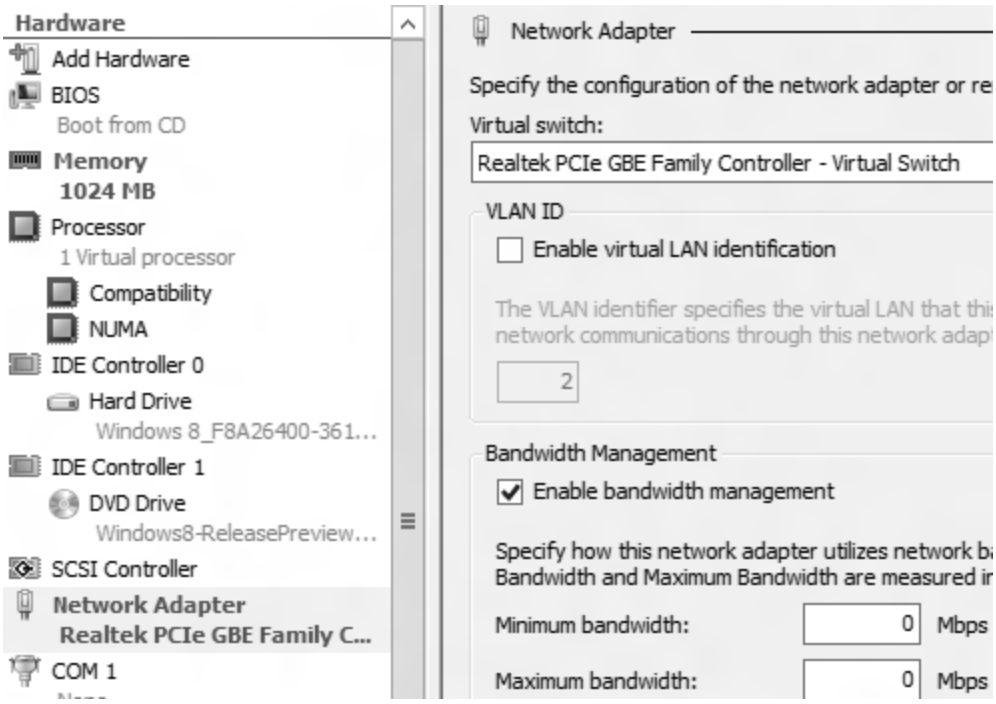
Pole niżej w menu to opcja NUMA, w ramach której określa się maksymalną ilość procesorów, z jakich maszyna może korzystać oraz maksymalną ilość pamięci operacyjnej.



Znajdują się także kontrolery IDE, do każdego z nich można podpiąć dwa urządzenia. Będzie to albo dysk twardy, albo napęd optyczny, do którego można podmontować obraz ISO lub fizyczny napęd gospodarza.



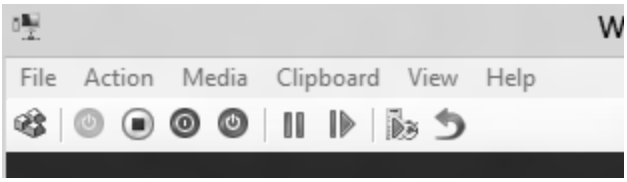
Poniżej znajdują się także ustawienia kontrolera sieci, gdzie można ustalić minimalną oraz maksymalną przepustowość adaptera w tej maszynie wirtualnej.



Przyciskiem OK należy zatwierdzić ustawienia i wrócić do Menadżera Hyper-V, w którym dwukrotnie należy kliknąć na utworzonej maszynie wirtualnej, a w oknie, które się pojawi, nacisnąć przycisk Start w celu uruchomienia komputera.

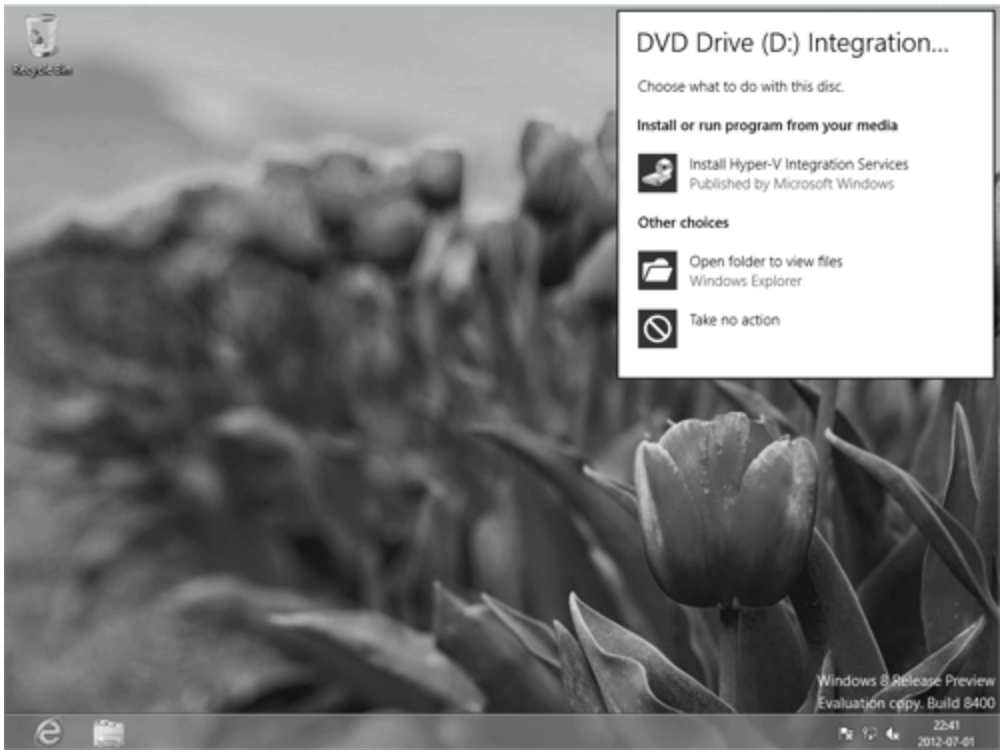
Załaduje się system operacyjny z płyty. Można na nim pracować tak, jak na zwykłym systemie operacyjnym. Natomiast myszkę, która zostanie uwięziona w oknie

maszyny wirtualnej, można uwolnić kombinacją klawiszy Ctrl + Shift + strzałka w lewo. W górnym menu obok przycisku Start znajduje się ikonka symbolizująca trzy guziczki, służąca do wysłania do maszyny wirtualnej kombinacji klawiszy Ctrl + Alt + Delete. Po prawej stronie guzika Start znajdują się kolejno: przycisk Turn Off powodujący wyłączenie maszyny wirtualnej, jednoznaczny z odłączeniem prądu, przycisk Shut Down, wysyłający sygnał wyłączenia do maszyny wirtualnej, przycisk Save pauzujący i zapisujący stan maszyny wirtualnej, przycisk Pause wstrzymujący maszynę wirtualną oraz przyciski Reset, Snapshot i Revert.



W górnym menu, po rozwinięciu przycisku Widok (View), istnieje możliwość uruchomienia maszyny w trybie pełnoekranowym. Przycisk Schowek (Clipboard) daje możliwość skopiowania do maszyny wirtualnej zawartości schowka oraz wykonania zrzutu ekranu maszyny wirtualnej. Pod przyciskiem Nośniki (Media) kryje się możliwość, szybszego niż przez ustawienia, podmontowania obrazu ISO lub napędu optycznego gospodarza. W menu Akcje (Action) znajdują się te same opcje, za które odpowiadają ikony. Istnieje także opcja Włóż dysk narzędzi integracji maszyny wirtualnej (Insert integration services setup disk), którą bezwzględnie należy uruchomić po zainstalowaniu systemu

operacyjnego w celu lepszego zintegrowania go z serwerem Hyper-V oraz wgrania sterowników.



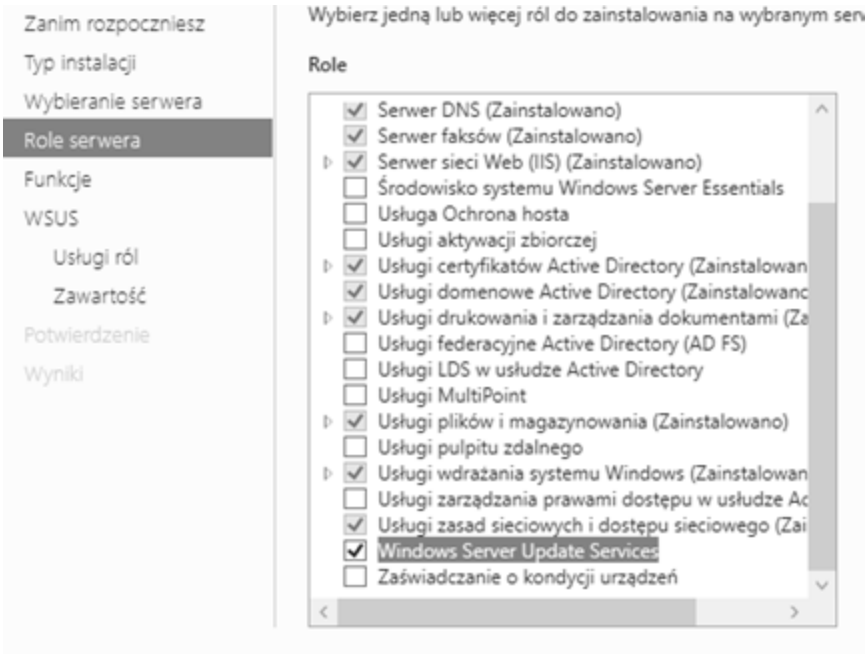
Nowością w Hyper-V jest także stworzenie nowej lokalnej grupy zabezpieczeń o nazwie Administratorzy Hyper-V (Hyper-V Administrators). Wystarczy dodać do niej użytkownika, aby ten miał pełen dostęp do funkcji Hyper-V.

16. Windows Server Update Services

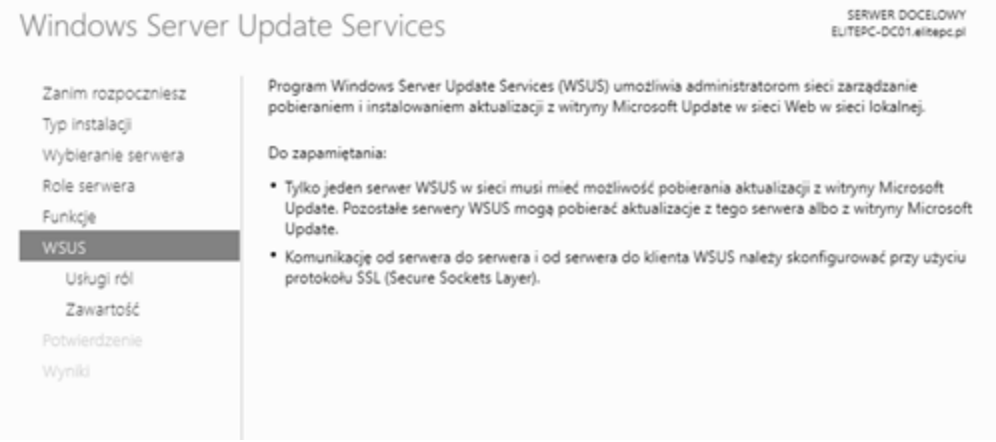
Należy dodać nową rolę do serwera, wybierając z listy Windows Server Update Services i następnie kliknąć Dalej(Next). Wymagany będzie IIS. Niniejsza usługa pobiera z oficjalnej witryny Microsoft Windows Update bądź z innego lokalnego serwera WSUS aktualizacje produktów Microsoft,

które zostaną wybrane w kreatorze konfiguracji. Następnie są one propagowane do innych komputerów w sieci tak, aby nie musiały one korzystać z oficjalnej witryny Windows Update i nadmiernie obciążać firmowych łącz.

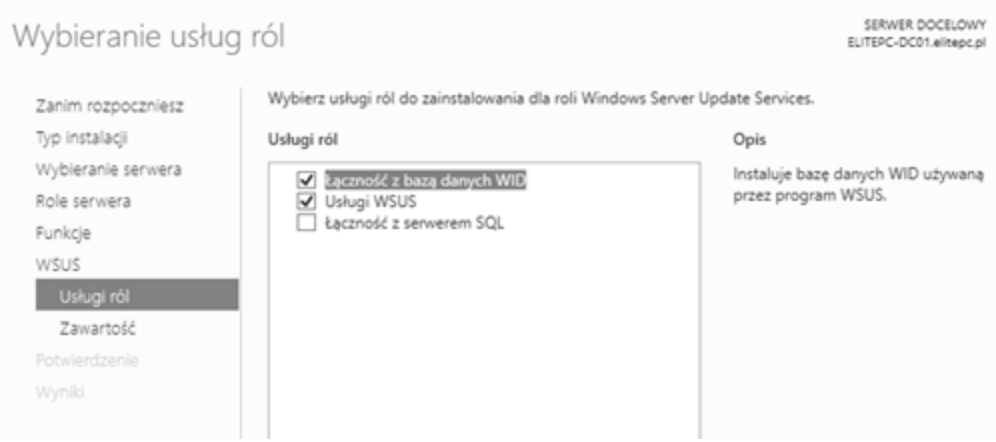
Po wybraniu Windows Server Update Services klika się Dalej (Next).



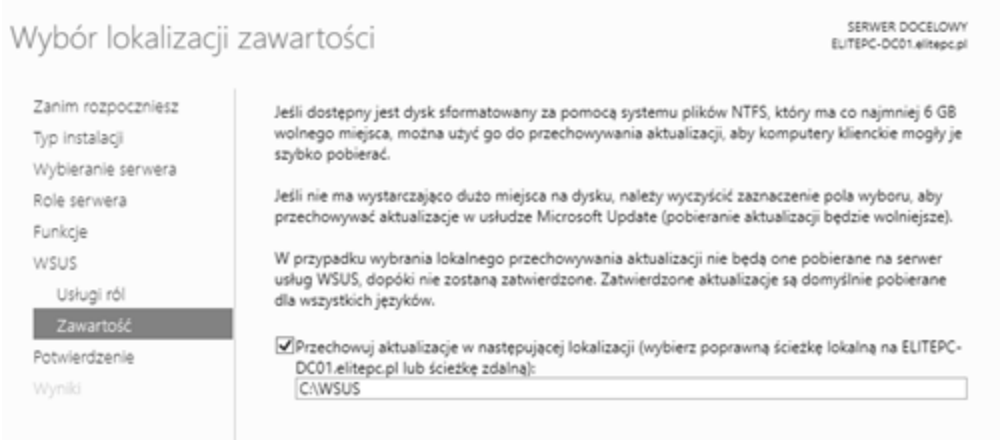
Karta powitalna kreatora informuje o tym, za co odpowiada serwer WSUS, a także o tym, jakie wymagania sieci muszą być zapewnione na maszynie hostującej tę rolę. Informuje również o tym, iż komunikacja pomiędzy komputerami klienckimi a serwerem oraz pomiędzy serwerami powinna być szyfrowana protokołem SSL.



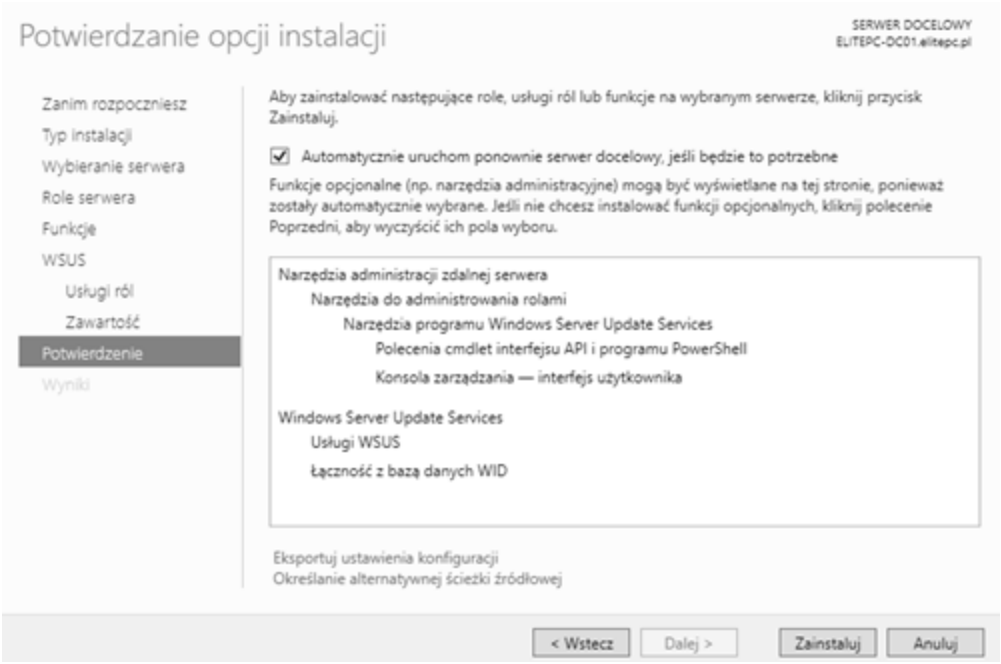
W kolejnym oknie kreatora należy wybrać składniki roli Windows Server Update Services, które powinny zostać zainstalowane. Niezbędne będą WSUS Services oraz jedna z baz danych (obu nie można zainstalować jednocześnie).



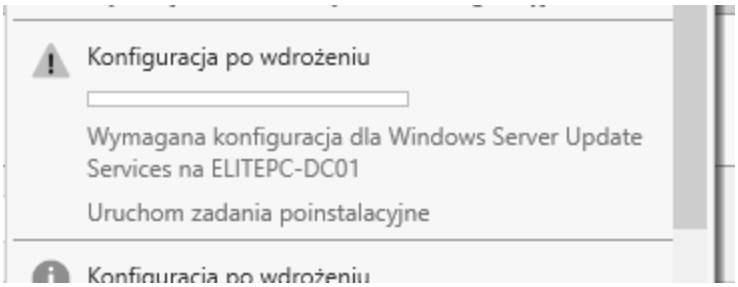
W kolejnym oknie kreatora należy podać miejsce, gdzie mają być przechowywane pobrane aktualizacje. Musi być to partycja o rozmiarze wynoszącym minimum 6 GB oraz sformatowana w systemie plików NTFS. Zaleca się użycie szybkiej macierzy dyskowej, aby wysyłać aktualizacje do maszyn klienckich bez opóźnień, o rozmiarze dostosowanym do ilości wybranych produktów Microsoft, dla których mają zostać pobrane aktualizacje.



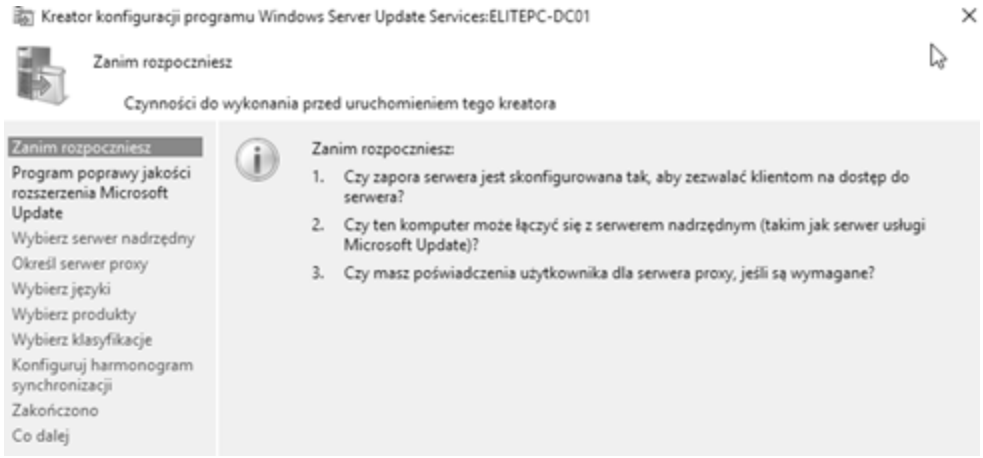
W oknie podsumowującym należy kontynuować instalację, klikając w przycisk Zainstaluj (Install).



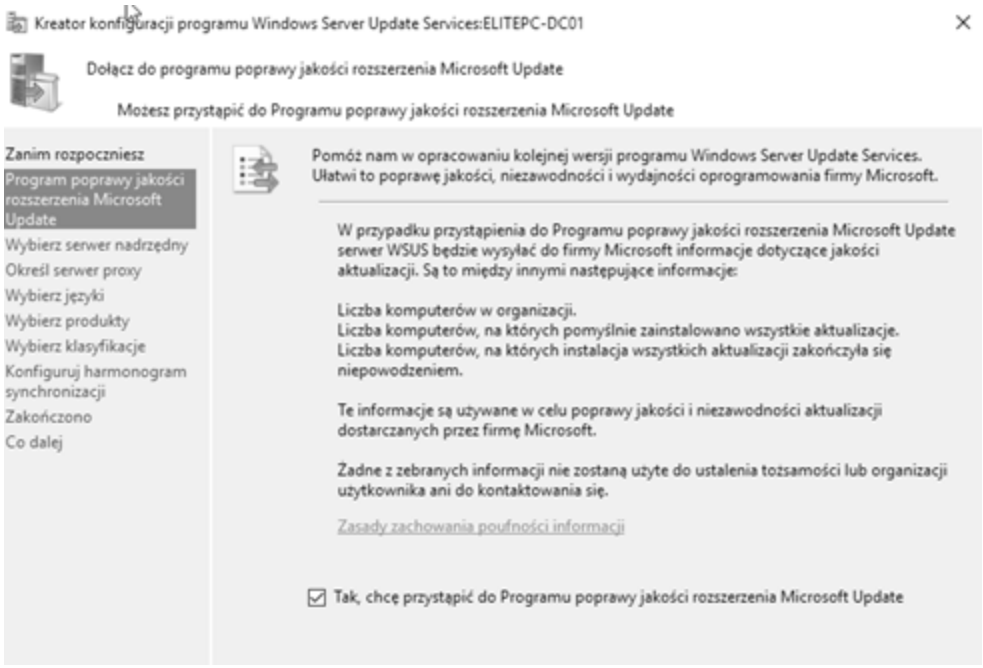
Gdy wszystkie wymagane pliki zostaną zainstalowane w Menadżerze Serwera, a dokładniej w Centrum Akcji należy kliknąć Uruchom czynności post instalacyjne (Launch Post Installation Tasks) w sekcji Konfiguracja powdrożeniowa (Post-deployment Configuration) dla Windows Server Update Services.



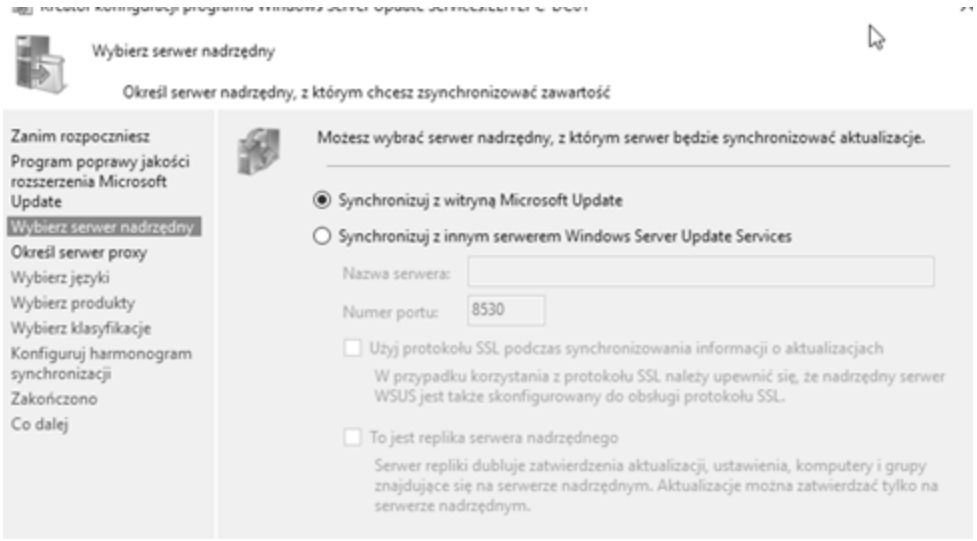
W ten sposób uruchomiony zostanie kreator konfiguracji roli, która właśnie została zainstalowana. Informuje on o tym, że zanim rozpocznie się proces konfiguracji, powinna zostać skonfigurowana zapora systemowa, tak aby umożliwiała klientom łączenie się z serwerem, a serwerowi na łączenie się z witryną Microsoft Windows Update, aby uzyskać informacje dotyczące serwera Proxy, jeżeli taki jest używany.



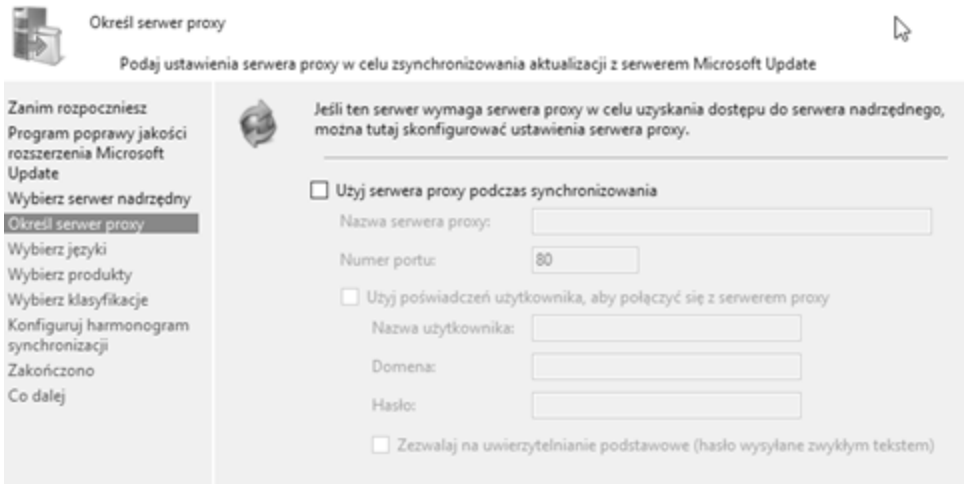
W kolejnym oknie kreatora można przystąpić do programu poprawy jakości produktów Microsoft, nie jest to jednak obligatoryjne.



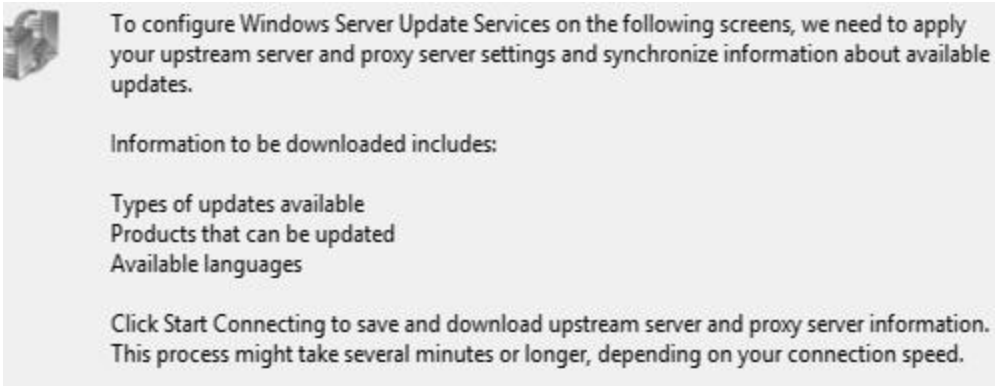
Następnie określa się, czy serwer ma się synchronizować z oficjalną witryną Microsoft Update, czy z innym serwerem WSUS.



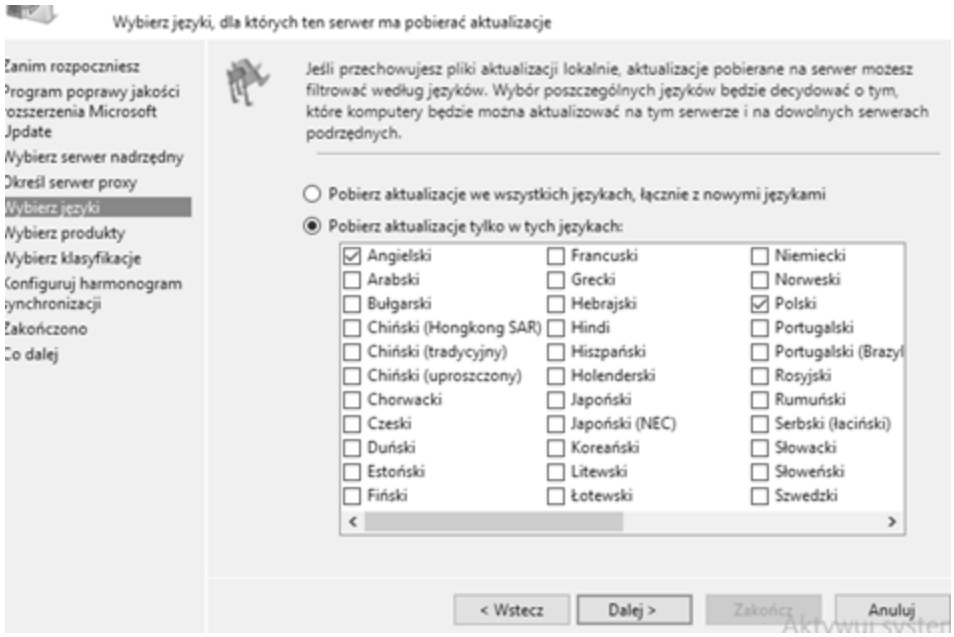
Kolejna karta kreatora to opcjonalne ustawienia serwera Proxy.



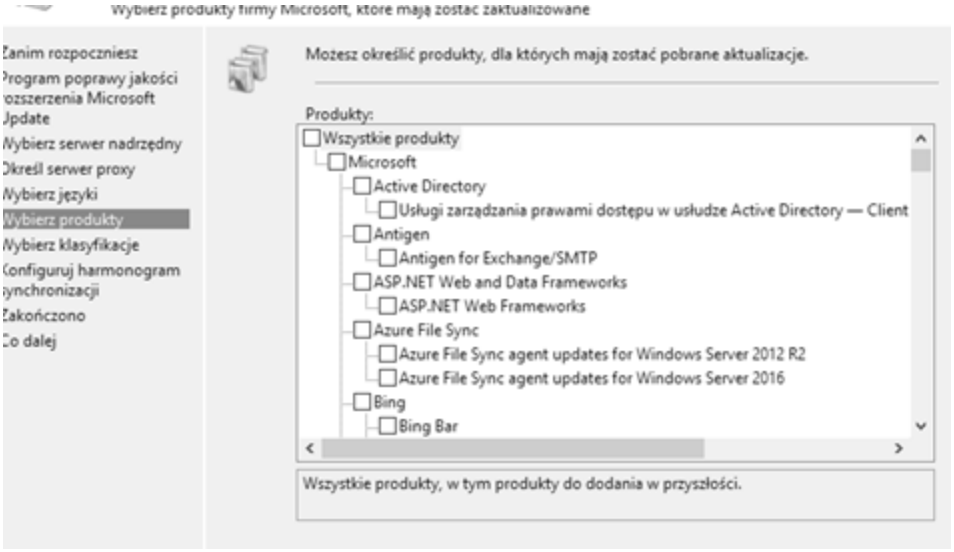
Następnie kreator spróbuje nawiązać połączenie z witryną Microsoft Update w celu pobrania informacji na temat rodzajów dostępnych aktualizacji, listy produktów, które mogą być aktualizowane oraz języków, w jakich te produkty są dostępne.



Gdy niezbędne informacje zostaną już pobrane w pierwszej kolejności należy wybrać języki produktów dla jakich będą pobierane aktualizacje.

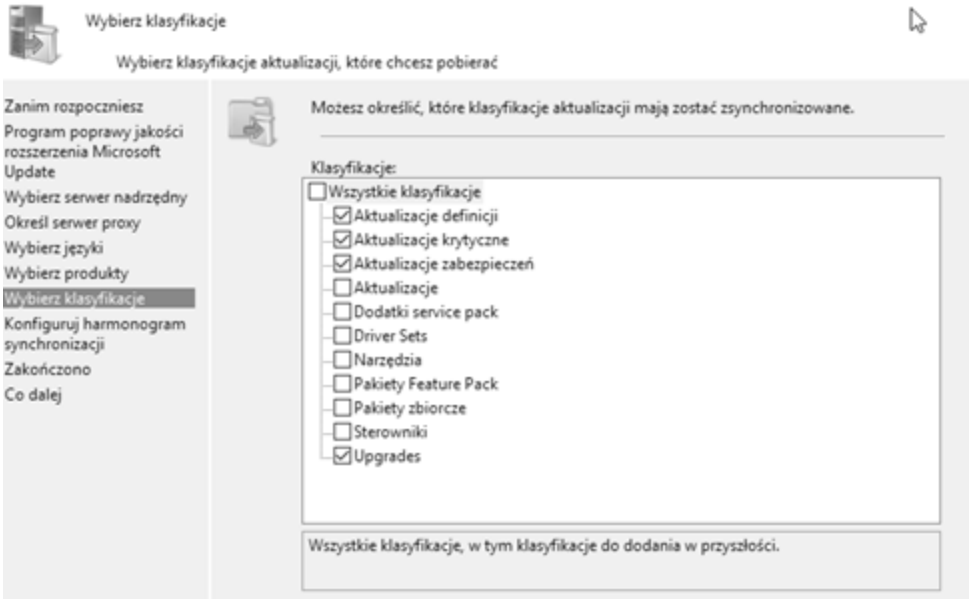


Po selekcji języków koniecznej jest wybranie z listy produktów, które są używane w przedsiębiorstwie, tak by pobierać wyłącznie te aktualizacje, które są niezbędne.

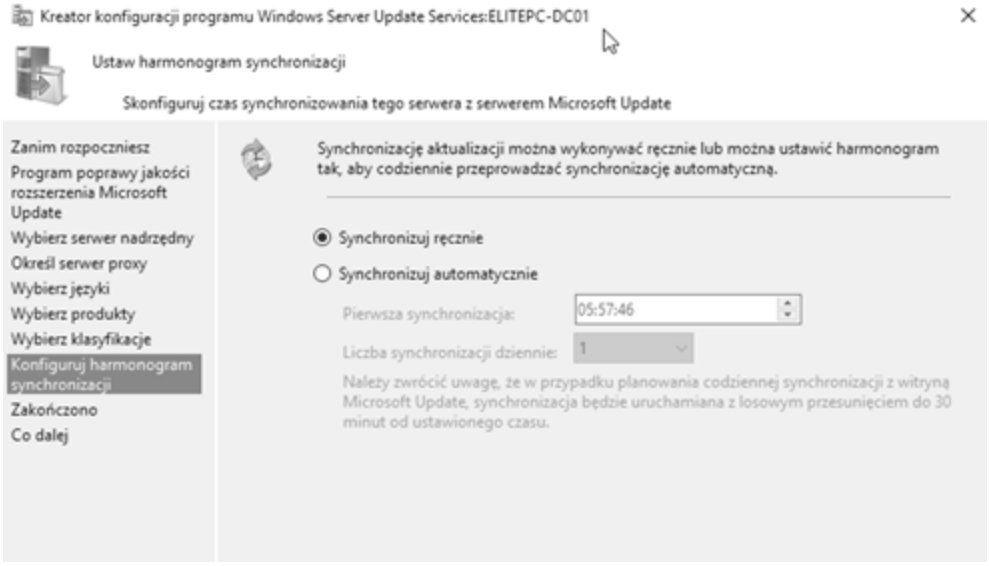


W kolejnym kroku określa się rodzaje aktualizacji, jakie mają być pobierane z witryny Microsft Update. Do wyboru są aktualizacje krytyczne, aktualizacje definicji, sterowniki, pakiety funkcji, aktualizacje zabezpieczeń, aktualizacje

zbiorcze Service Pack, narzędzia, aktualizacji Rollupów oraz zwykłe aktualizacje.

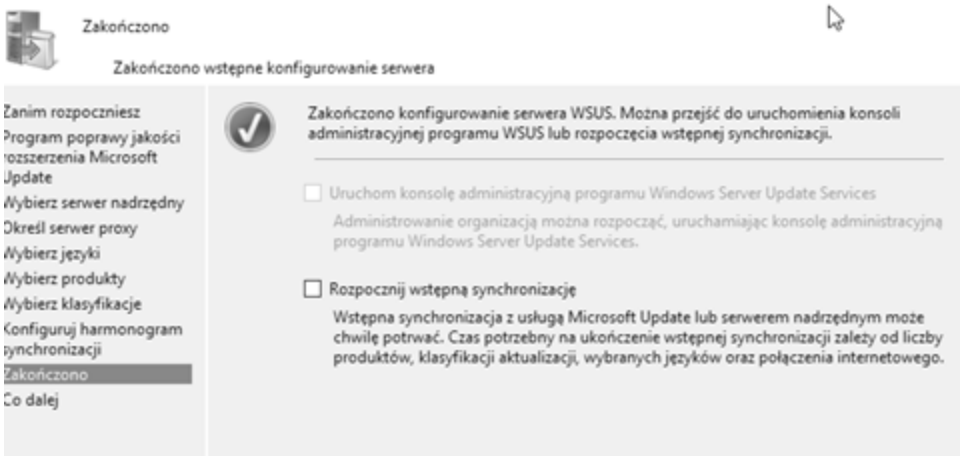


Gdy uda się przefiltrować pożądane pliki do pobrania, należy określić, czy serwer WSUS będzie synchronizowany z witryną Windows Update ręcznie, czy automatycznie. Zaleca się, aby aktualizacje pobierać w godzinach nocnych.

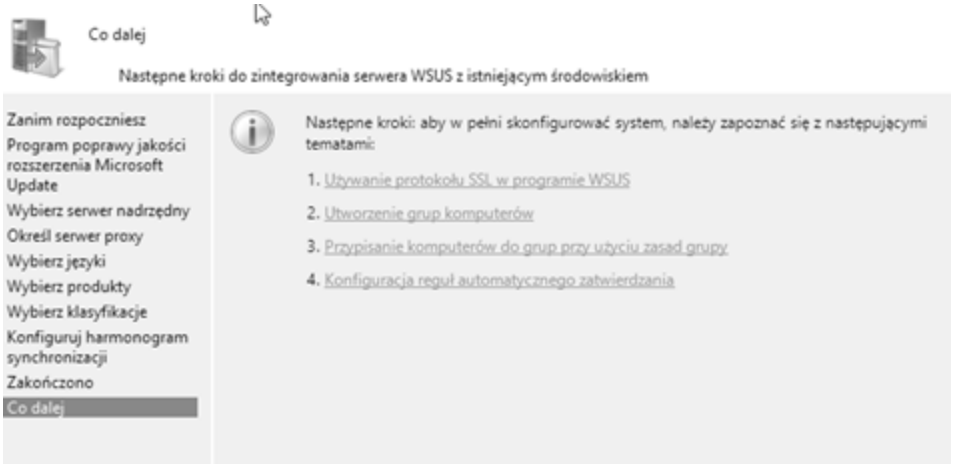


Kończąc kreator konfiguracji opcją Rozpocznij pierwszą synchronizację (Begin initial synchrozation) można

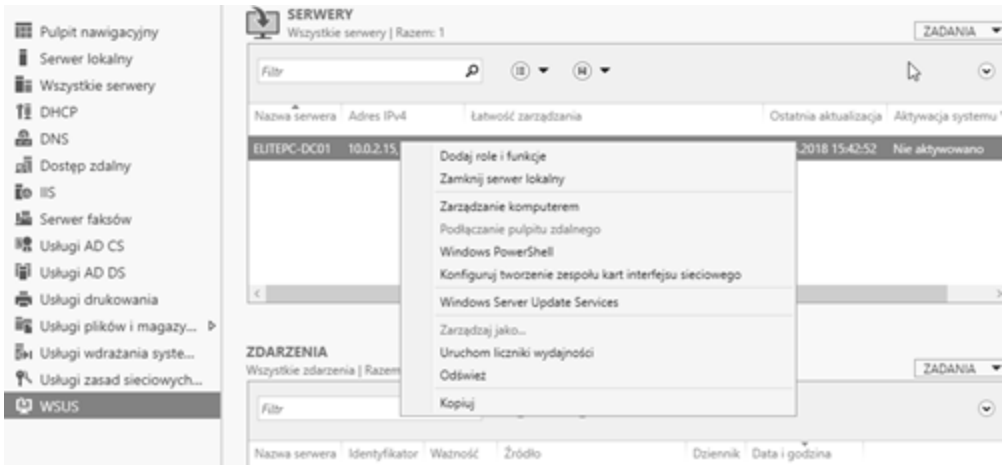
rozpocząć wstępną synchronizację. Z racji tego, że do pobrania będzie pokaźna ilość danych, należy uzbroić się w cierpliwość.



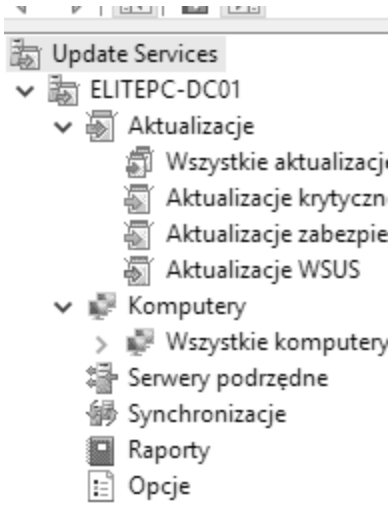
W karcie podsumowującej należy kliknąć Zakończ (Finish).



Po zakończeniu kreatora rola WSUS pojawi się w Menadżerze Serwera, aby nią zarządzać, należy na wybranym serwerze kliknąć prawym przyciskiem myszy i wybrać Windows Server Update Services.

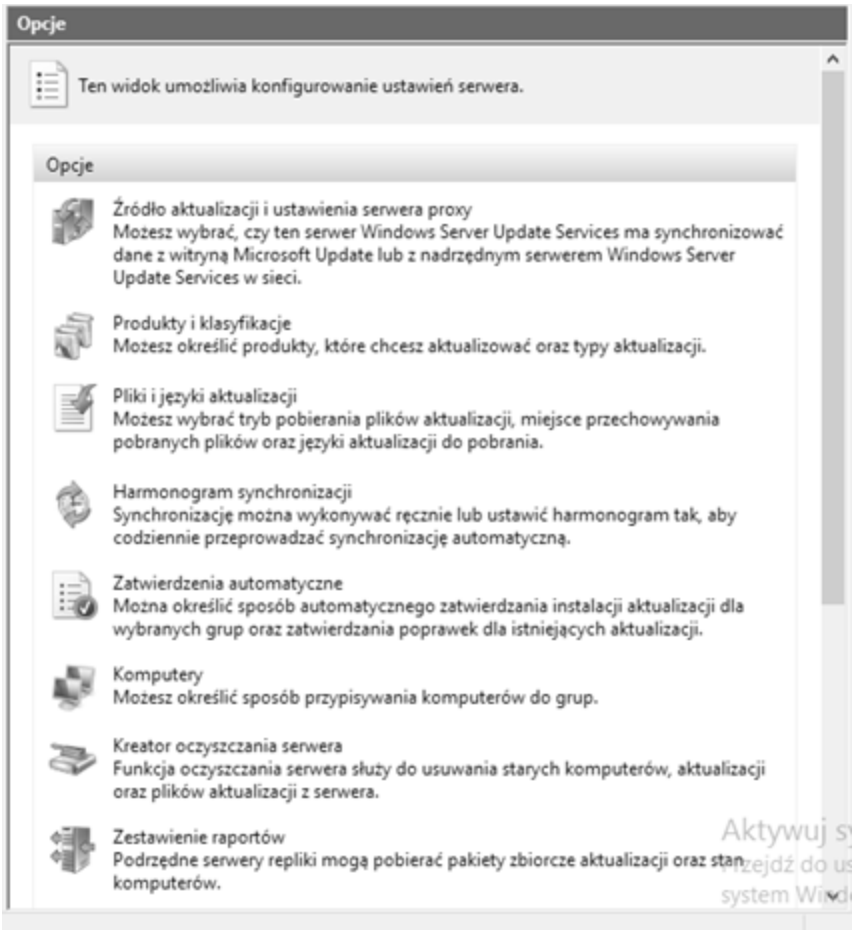


W konsoli zarządzania rolą Windows Server Update Services warto szczególną uwagę zwrócić na Opcje (Options).

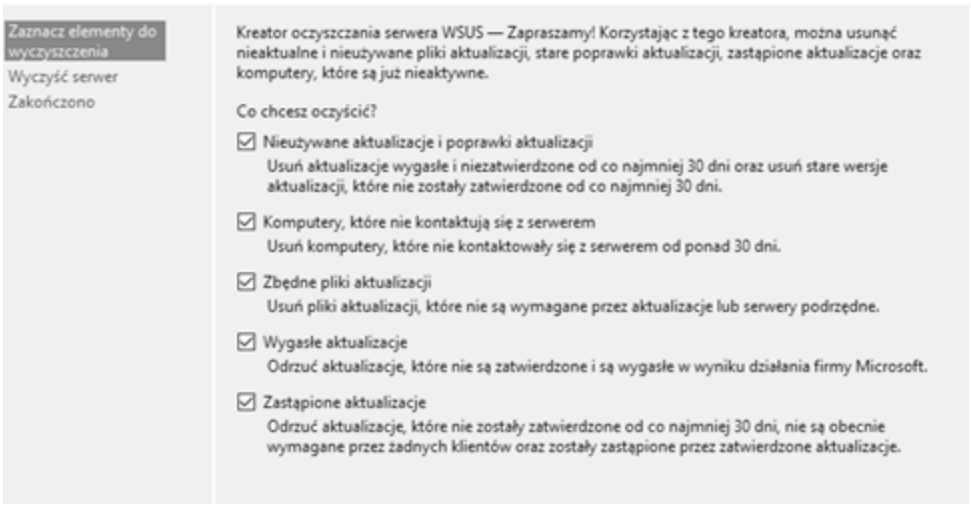


W tym miejscu znajdują się dodatkowe ustawienia WSUS. Opcja Automatic Approvals pozwala określić, jak automatycznie zatwierdzić instalację aktualizacji dla wybranych grup. Sychronization Schedule pozwala zarządzać automatycznymi synchronizacjami, bądź synchronizować się manualnie. Computers określa, w jaki sposób maszyny przypisywane są do grup. Warto także zaznajomić się z innymi ustawieniami. Na szczególną uwagę

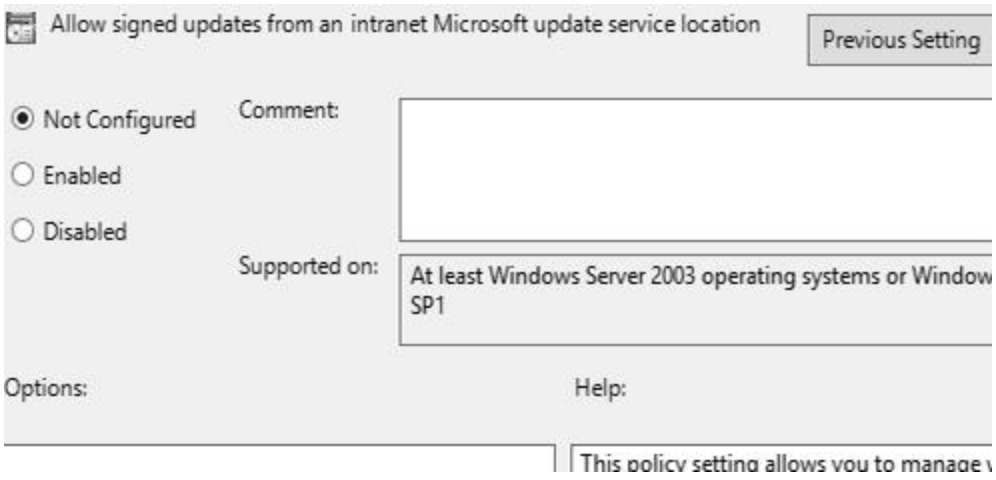
zasługuje Server Cleanup Wizard, czyli kreator oczyszczania serwera.



Kreator oczyszczania serwera pozwala na automatyczne kasowanie nieużywanych i nieaktualnych plików. W oknie, które się pojawi, określa się elementy, które mają zostać oczyszczone.



Gdy WSUS jest odpowiednio skonfigurowany, należy zadbać o rzecz najważniejszą, czyli o to, aby maszyny klienckie wiedziały, że mają korzystać z tego serwera zamiast oficjalnej witryny Microsoft Update. Aby wymusić aktualizację z lokalnego serwera, należy dokonać odpowiedniej edycji polisy związanej z intranetową witryną Windows Update. W anglojęzycznej wersji systemu Windows Server 2016 nosi ona nazwę Allow signed updates from an intranet Microsoft updates service location.



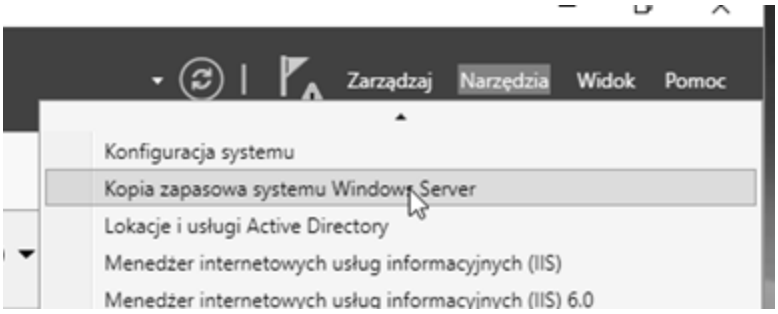
17. Bezpieczeństwo danych i komputera

Backup to rzecz podstawowa w pracy administratora. Dane, jak i same systemy, trzeba nieustannie archiwizować na bezpiecznych nośnikach danych.

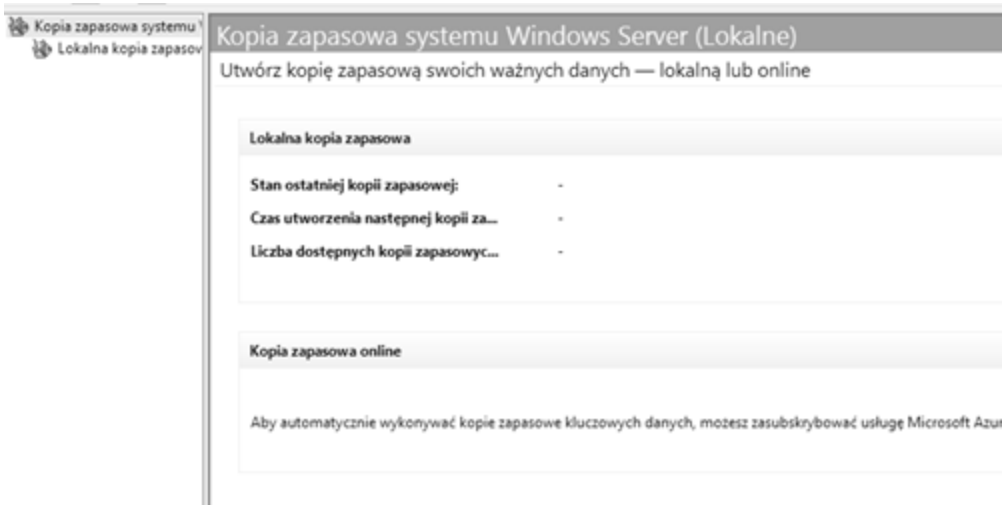
17.1. Windows Backup

Do serwera należy dodać funkcję Kopia zapasowa systemu Windows Serwer (Windows Server Backup) i kliknąć Dalej (Next). Resztę instalacji przechodzi się analogicznie do instalacji innych ról.

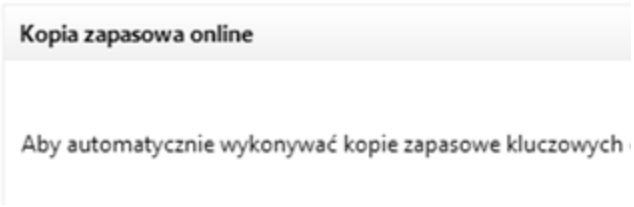
Po zainstalowaniu powyższej funkcji można teraz wejść w Narzędzia Administracyjne > Kopia zapasowa Systemu Windows Serwer (Tools > Windows Server Backup).



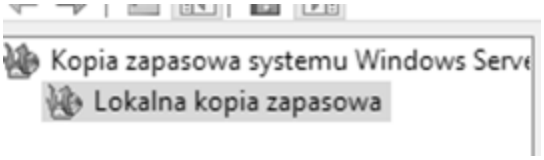
Uruchomiona w ten sposób zostanie konsola kopii zapasowej w systemie Windows Server.



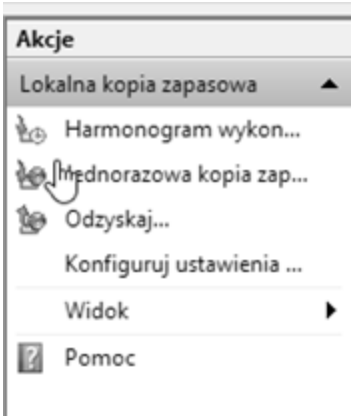
Kopię zapasową można wykonywać standardowo na nośnikach lokalnych. Nowością w Windows Server 2016 jest możliwość kopii zapasowej danych w chmurze.



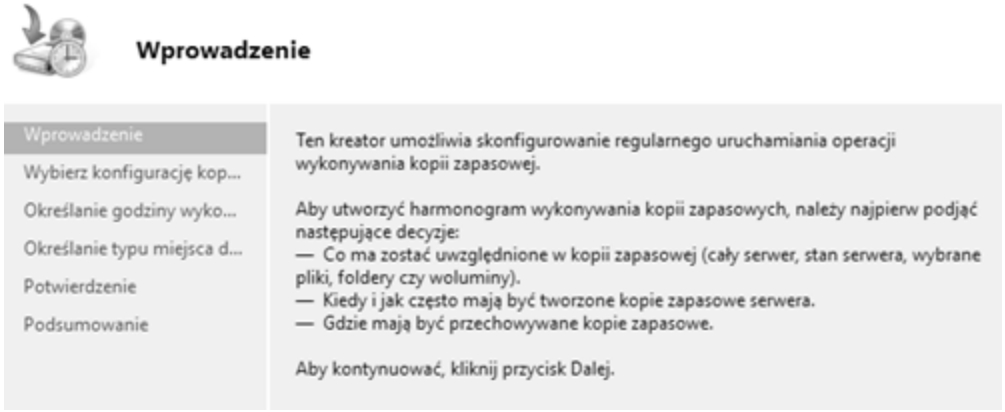
W drzewie po lewej stronie znajdują się listy dostępnych kopii zapasowych.



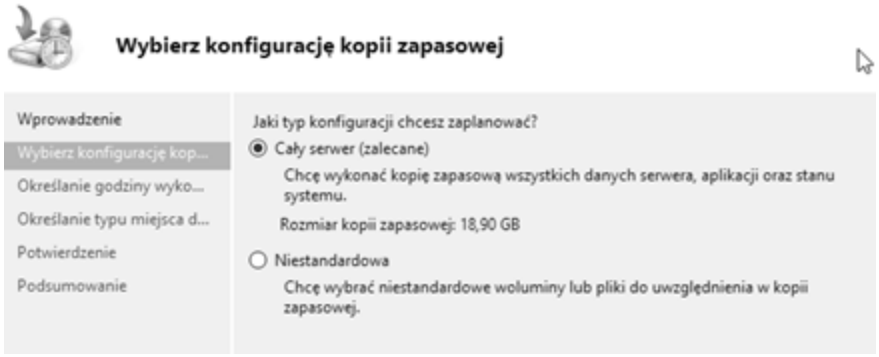
Należy kliknąć w opcję Harmonogram wykonywania (Backup Schedule), która znajduje się w prawym panelu na samej górze.



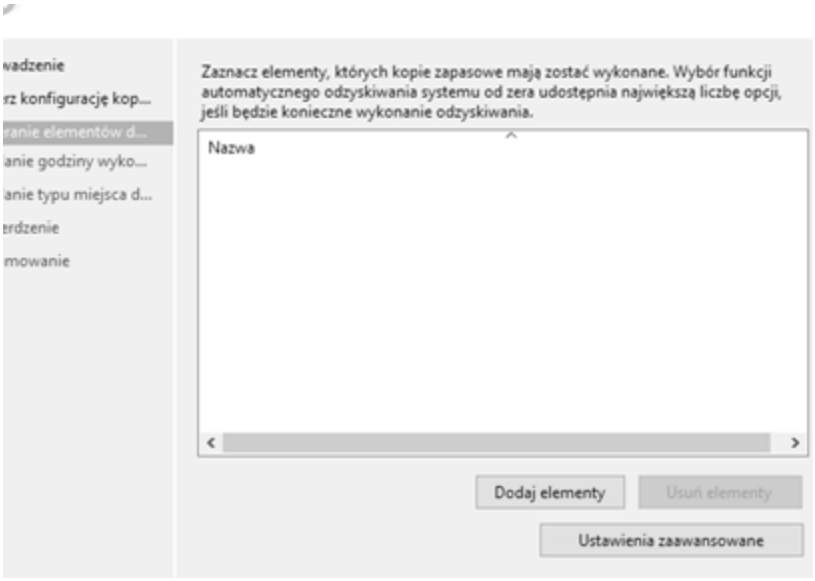
Otworzy się kreator harmonogramu wykonywania kopii zapasowych, w którym zachodzi potrzeba kliknięcia przycisku Dalej (Next).



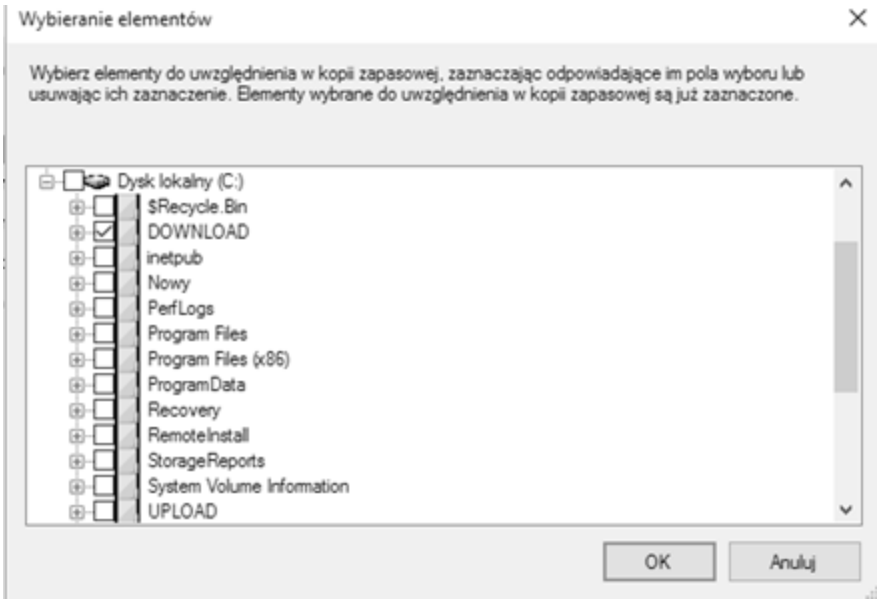
Następnie należy wybrać Konfigurację Niestandardową (Custom) i kliknąć Dalej (Next).



Należy kliknąć Dodaj Elementy (Add Items), dzięki czemu możliwe jest dodanie tylko określonych elementów do skopiowania, zamiast wykonywania kopii całego serwera. Jest to przydatne, gdy administrator pragnie przechowywać różnego rodzaju dane w różnych bezpiecznych lokalizacjach.

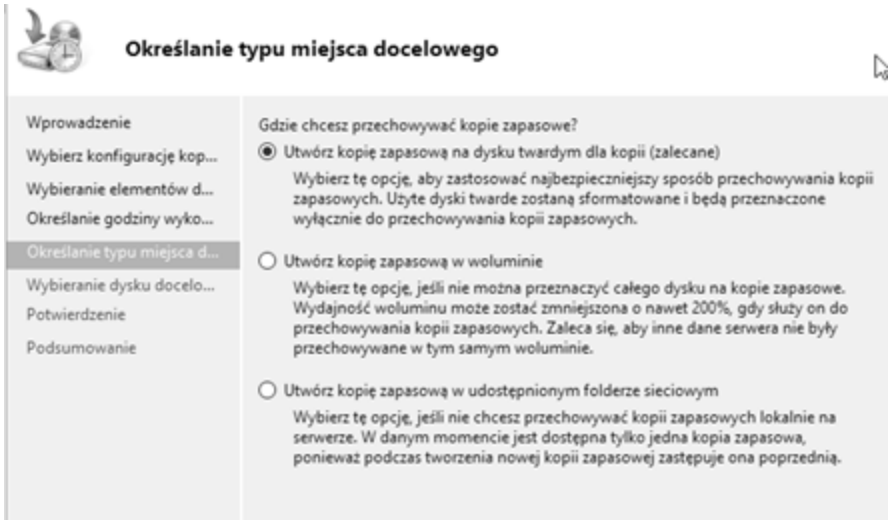


Na kolejnej karcie wybiera się elementy do wykonania kopii zapasowej.



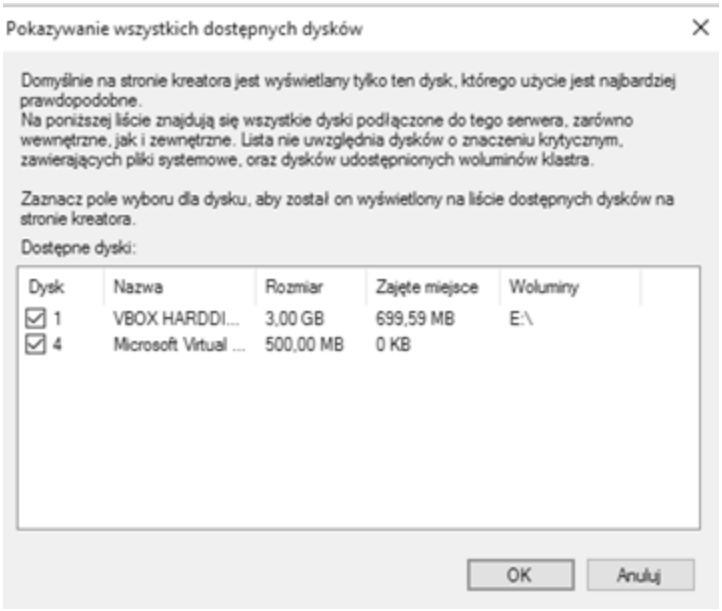
W następnym kroku należy określić harmonogram wykonywania kopii, czyli w jakich godzinach ma być wykonana kopia zapasowa.

Następnie należy określić typ miejsca docelowego. Do wyboru jest kopia na dysku lokalnym (Back up to a hard disk that is dedicated for backups), na woluminie (Back up to a volume) oraz w lokalizacji sieciowej (Back up to a shared network folder).



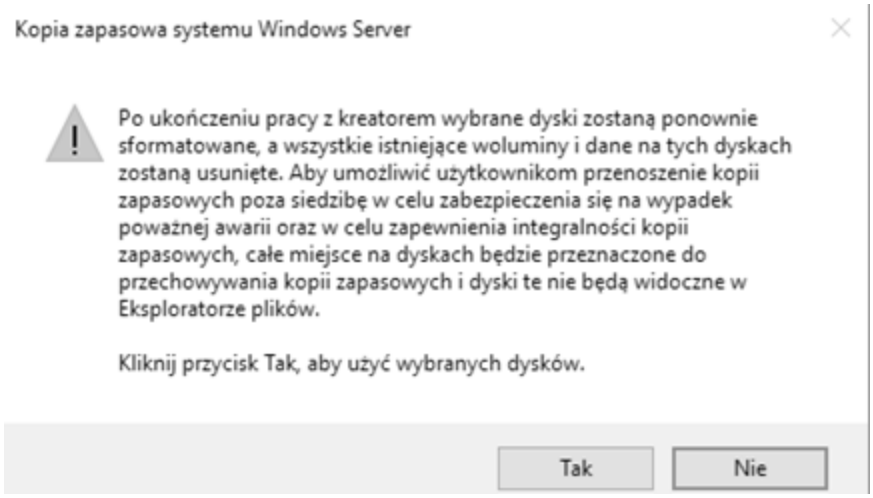
Jeżeli administrator zdecyduje się na wykorzystanie całych dysków, w zależności od ich ilości, kreator połączy je w macierz Raid oraz je sformatuje i przygotuje do przechowywania kopii zapasowej.

W ćwiczeniowym, wirtualnym środowisku znajdują się dwa dyski po 500 MB każdy. Można zaznaczyć wszystkie dyski i kliknąć OK.

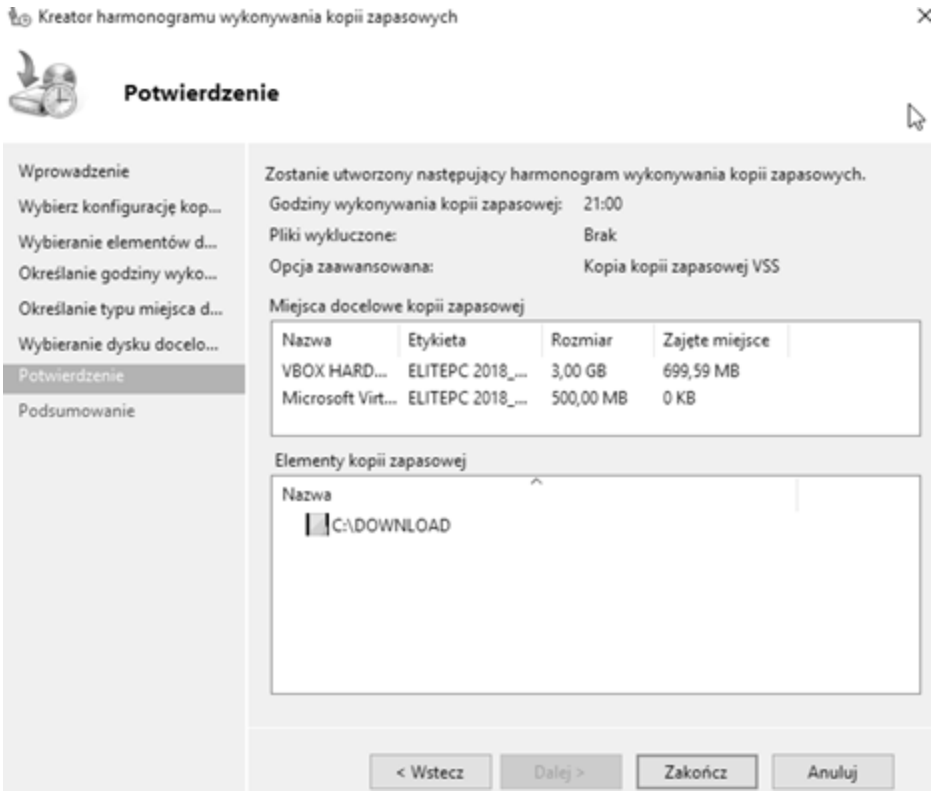


Na komunikacie, który się pojawi, należy kliknąć Tak (Yes). Informuje on czytelnika o tym, iż wybrane dyski

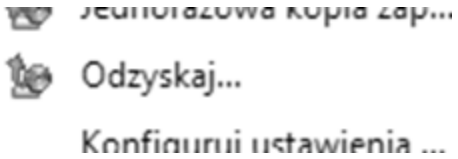
zostaną sformatowane, a dane już na nich zebrane zostaną utracone.



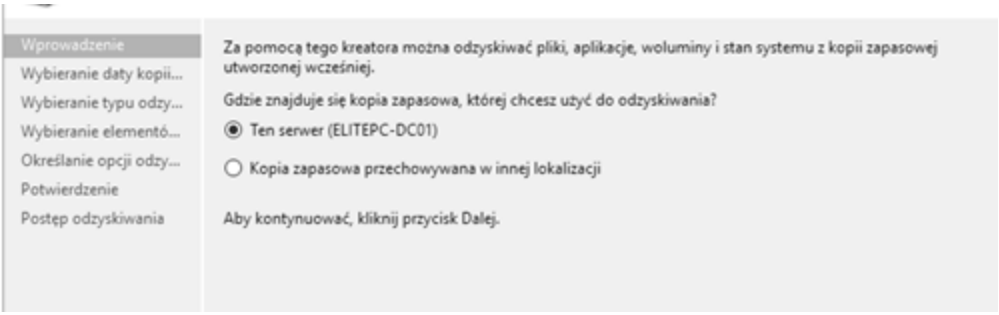
Następnie należy potwierdzić kartę podsumowującą kreatora, klikając Zakończ (Finish).



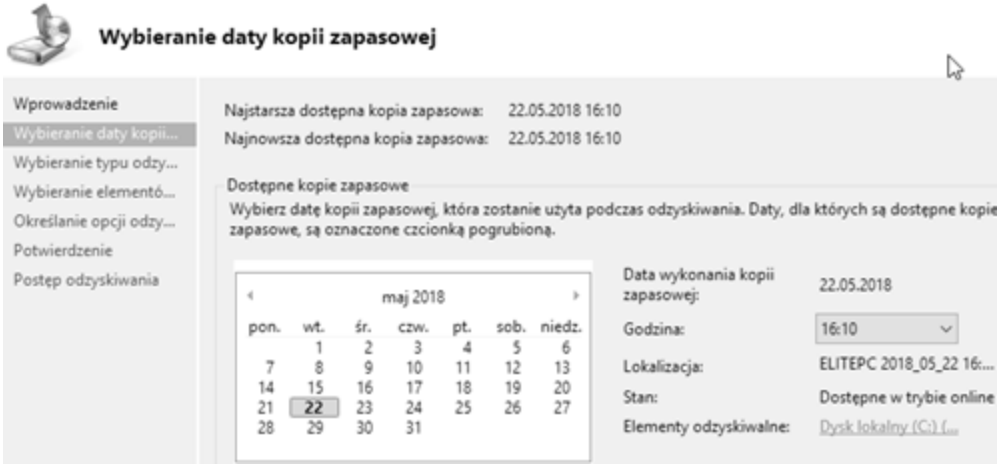
W celach treningowych można odzyskać dane. Należy więc kliknąć Odzyskaj (Recover).



Otworzy się kreator odzyskiwania, w którym należy wybrać lokalizację, w jakiej przechowywana jest kopia, oraz kliknąć Dalej (Next). Do wyboru jest kopia na Lokalnym serwerze (This server) oraz w Innej lokalizacji (A backup stored on another location).

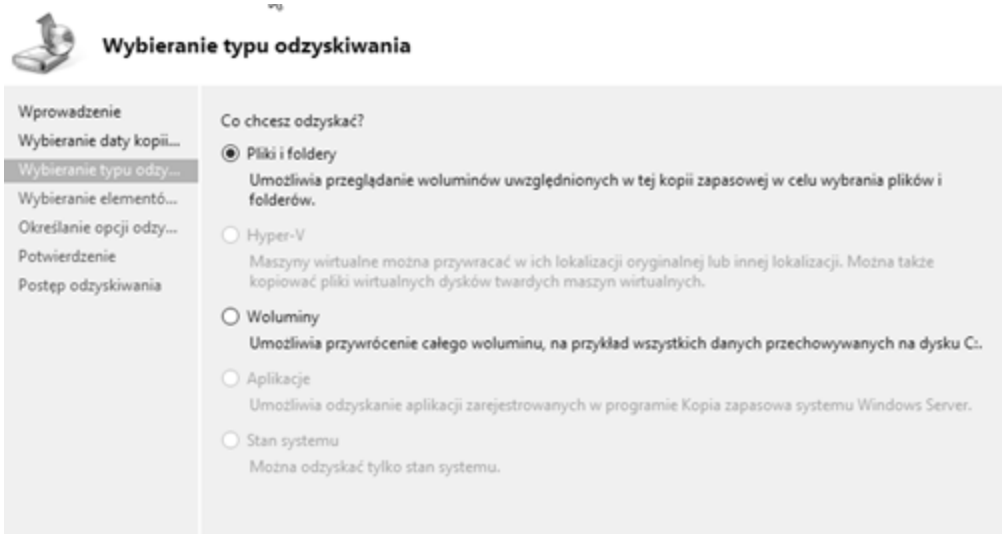


Następnie wybiera się datę, z kiedy mają zostać przywrócone pliki.

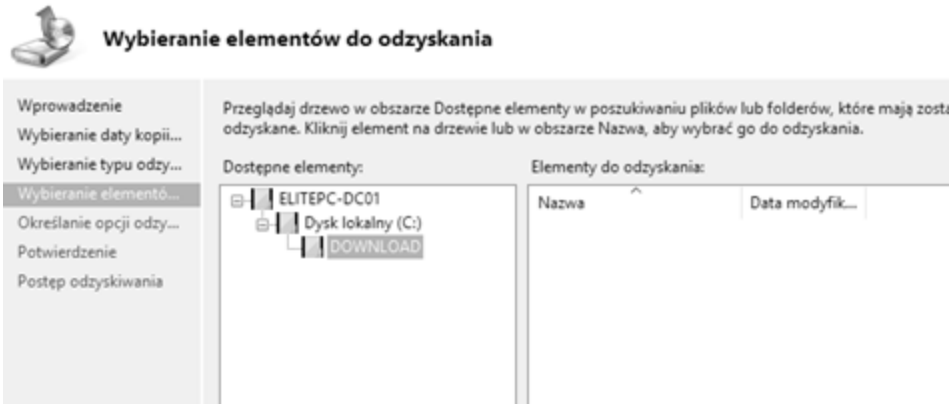


Należy wybrać typ odzyskiwania i kliknąć Dalej (Next). Do wyboru jest Odzyskiwanie plików i folderów (Files and folders), gdzie administrator może ręcznie wybrać pojedyncze pliki lub folder, Przywracanie maszyn wirtualnych Hyper-V (Hyper-V), przywracanie całych

Woluminów (Volumes) oraz Aplikacji (Applications). Można także przywrócić wcześniej zapisany stan systemu operacyjnego.

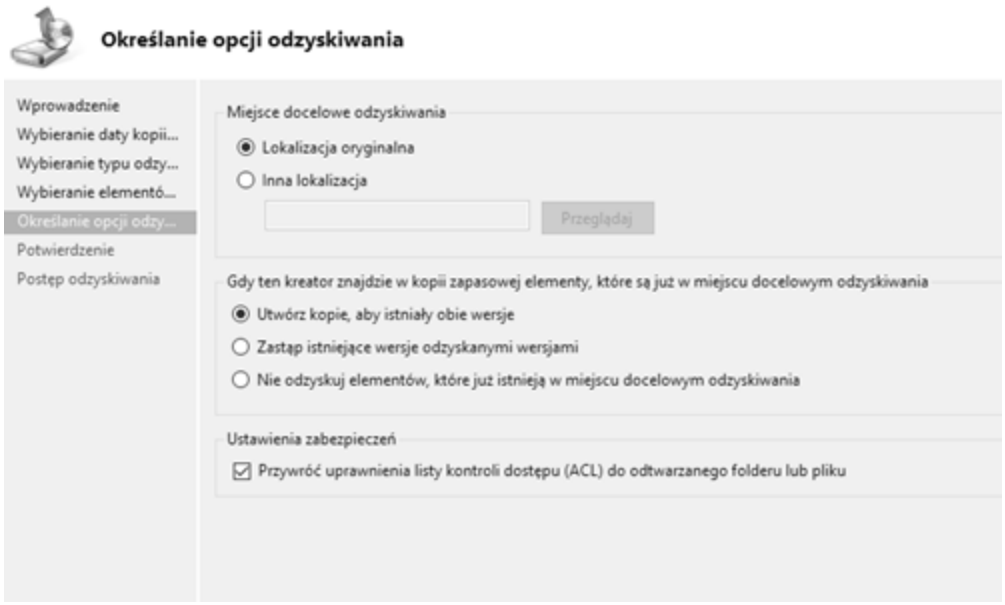


Po wybraniu pierwszej opcji, tj. Przywracanie pojedynczych plików i folderów (Files and folders), należy zaznaczyć elementy do odzyskania i kliknąć Dalej (Next).

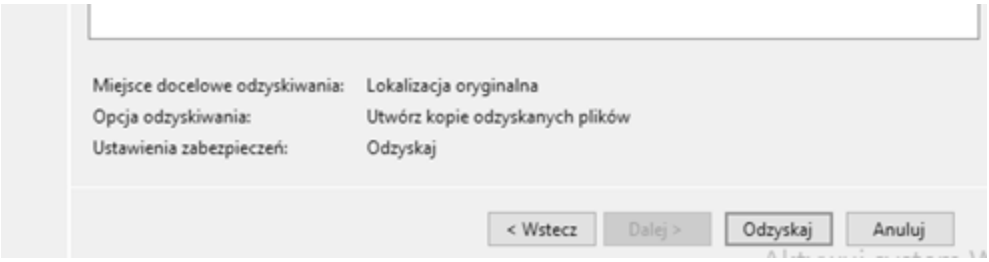


W kolejnym kroku określa się opcje odzyskiwania. Przede wszystkim należy określić, czy dane mają być odzyskane w swoim oryginalnym miejscu, a co za tym idzie, nowe pliki zostaną nadpisane, czy też w lokalizacji alternatywnej, co pozwoli zachować obie wersje plików. Należy także określić, jak ma się zachować kreator, jeżeli w docelowej lokalizacji

napotka już jakieś wersje plików oraz to, co ma on zrobić z uprawnieniami ACL.



Na karcie podsumowującej należy użyć przycisku Przywróć (Recover), aby rozpocząć przywracanie plików.



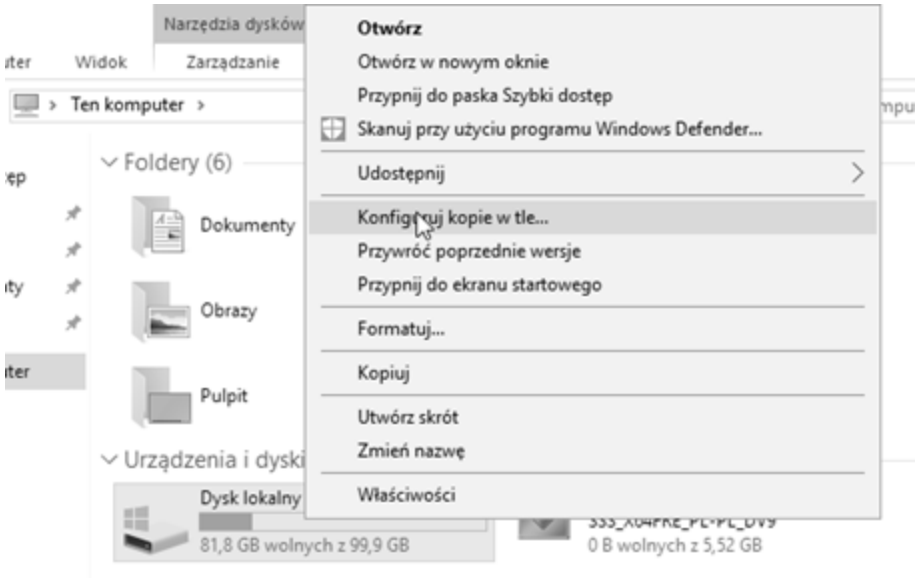
17.2. Shadow Copies

Funkcja kopiowania w tle (Shadow Copies) folderów udostępnionych umożliwia tworzenie bieżących kopii plików należących do zasobów udostępnionych, takich jak serwer plików. Dzięki tej funkcji można przeglądać udostępnione

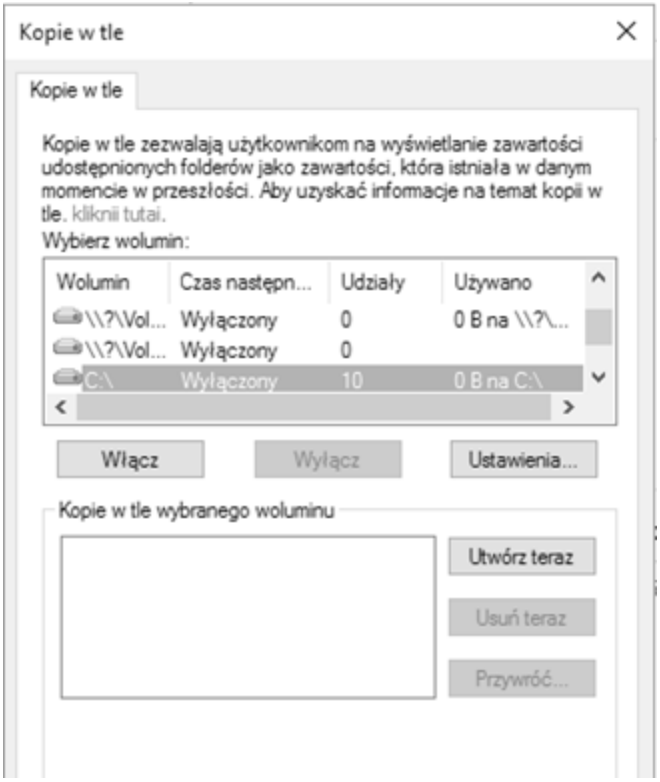
pliki i foldery w stanie, w jakim znajdowały się w określonym czasie w przeszłości.

Za pomocą funkcji kopiowania w tle (Shadow Copies) można odzyskiwać pliki, które zostały przypadkowo usunięte lub zastąpione oraz porównywać różne wersje plików.

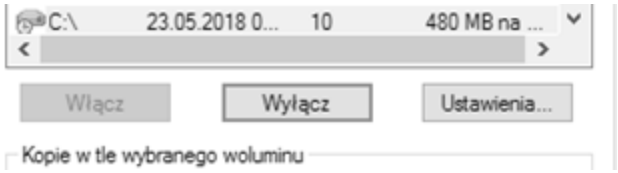
W celu ich uruchomienia należy otworzyć Mój Komputer i kliknąć prawym przyciskiem myszy na lokalnym dysku komputera, a następnie wybrać Konfiguruj Kopie w tle (Configure Shadow Copies).



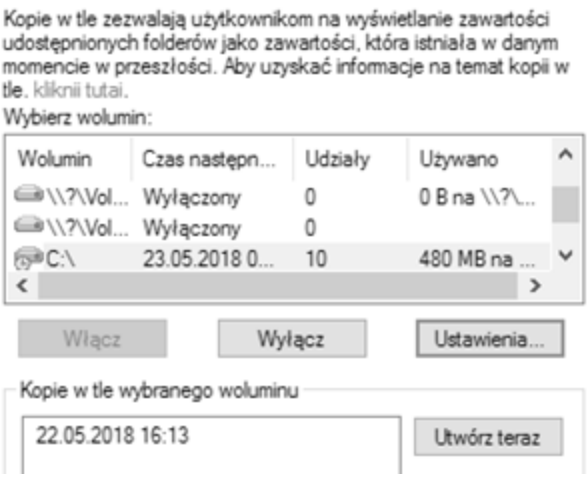
Następnie należy kliknąć w wybrany wolumin i wybrać opcję Włącz (Enable). Spowoduje to uruchomienie na nim kopii w tle. Za chwilę przeprowadzony zostanie demonstracyjny proces, który ma na celu pokazanie, w jaki sposób działają kopie w tle, jak z nich korzystać oraz jak je prawidłowo skonfigurować.



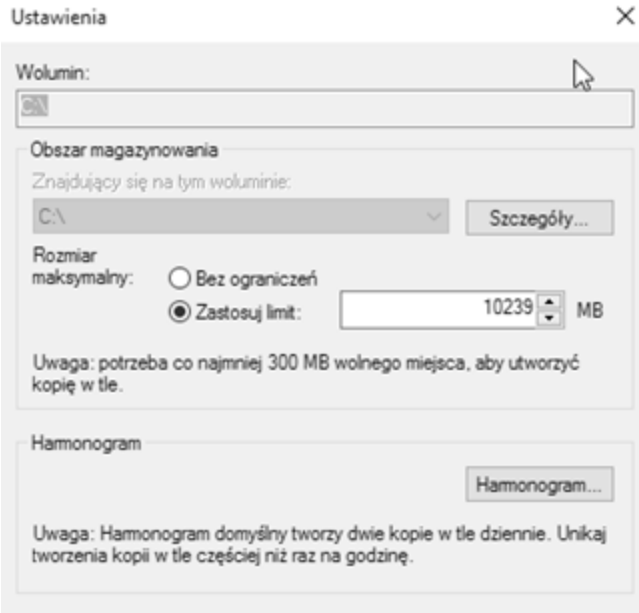
Należy kliknąć Tak (Yes) na komunikacie, jaki się pojawi. Informuje on o tym, iż nie zaleca się uruchamiania kopii w tle na maszynach o dużym obciążeniu.



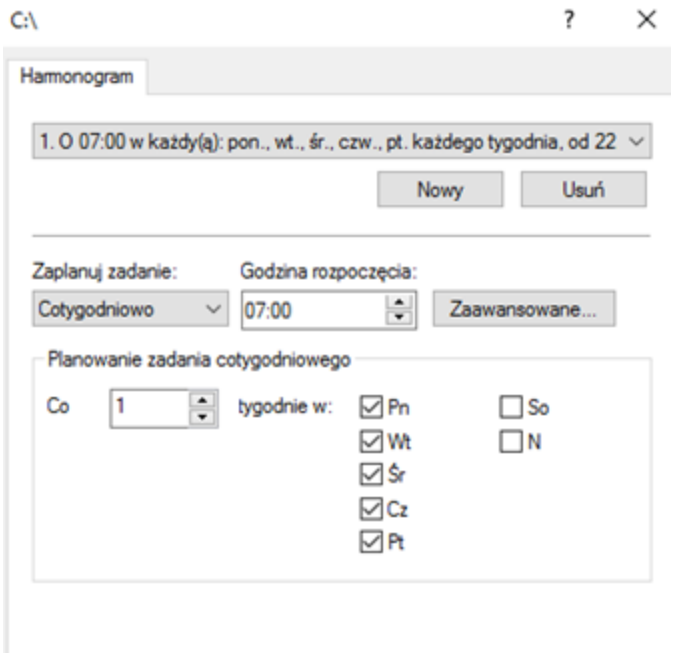
Następnie konieczne jest wejście w Ustawienia (Settings) w celu dokonania dalszej konfiguracji, m.in. ustawienia harmonogramu wykonywania kopii.



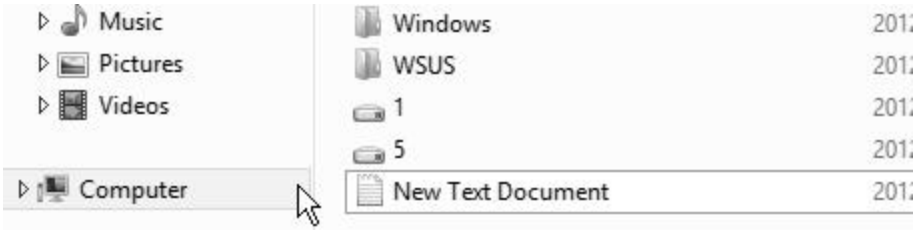
W następnym kroku ustawia się na dysku limit miejsca, jakie będzie zarezerwowane dla kopii w tle, np. wynoszący 600 MB. Gdy limit zostanie osiągnięty, kasowane będą najstarsze wersje plików. Później należy wybrać Harmonogram (Schedule).



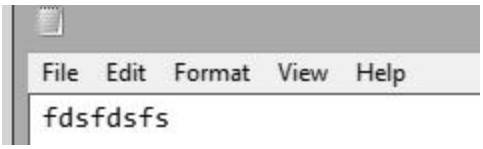
Harmonogram określa, jak często wykonywana jest kopia plików, które uległy zmianie. Można np. wybrać wykonywanie kopii przy logowaniu, dzięki czemu użytkownicy zawsze będą mieli dostęp do swoich plików z poprzedniego dnia pracy.



W celu przeprowadzenia pokazu działania kopii w tle, należy na wcześniej wybranym woluminie utworzyć nowy dokument tekstowy.

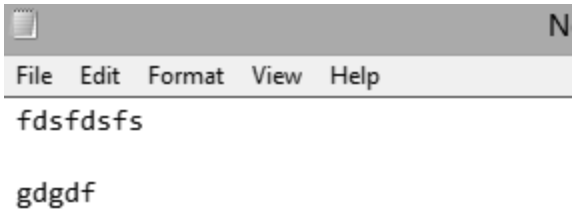


Następnie w utworzonym dokumencie należy wprowadzić jakąkolwiek treść.

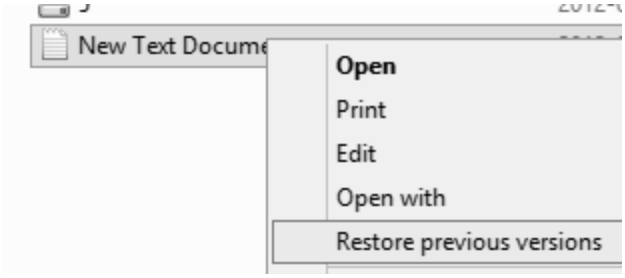


Na karcie konfiguracyjnej kopii w tle można kliknąć Utwórz teraz (Create Now), co spowoduje wymuszenie wykonania kopii w tle.

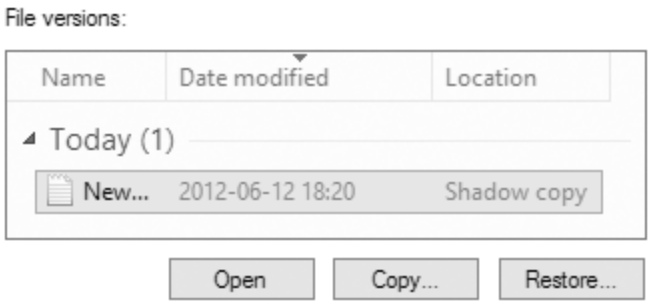
Czynności te należy powtórzyć wielokrotnie po to, aby utworzyć kilka wersji tego samego pliku.



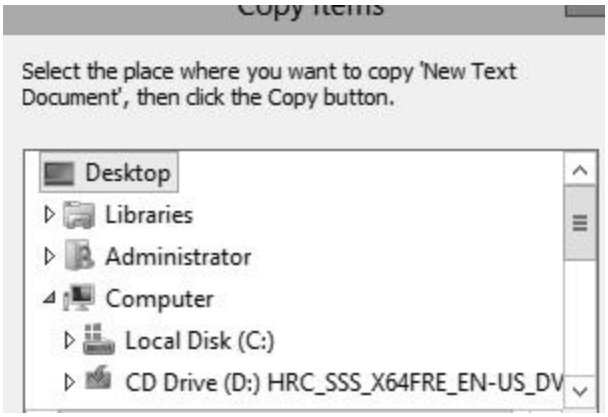
Gdy kopie są już przygotowane, użytkownik na komputerze łączącym się do swojego zasobu będzie miał pod prawym klawiszem myszy opcję Przywróć poprzednie wersje (Restore previous versions). Należy w nią kliknąć.



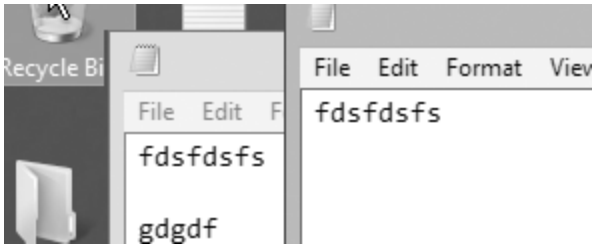
W oknie, które się pojawi, można wybrać dowolną poprzednią wersję pliku.



Poprzedni plik użytkownik może otworzyć w celu podglądu, skopiować w dowolne inne miejsce lub przywrócić w jego oryginalnej lokalizacji, co spowoduje nadpisanie najnowszej wersji pliku.



Jak widać, została przywrócona poprzednia wersja pliku sprzed edycji treści.

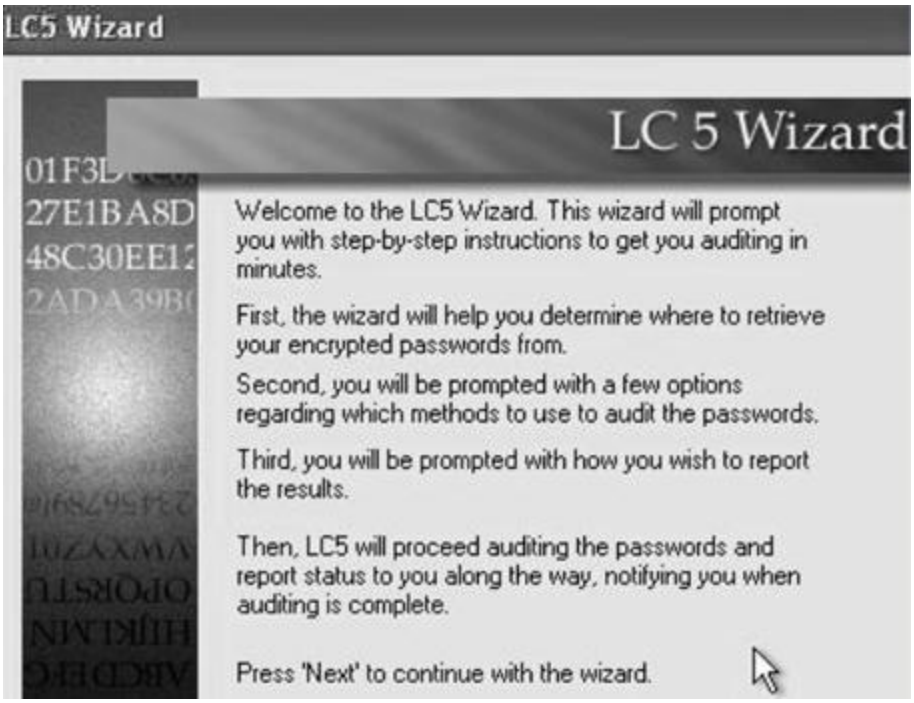


17.3. Kilka uwag ogólnych

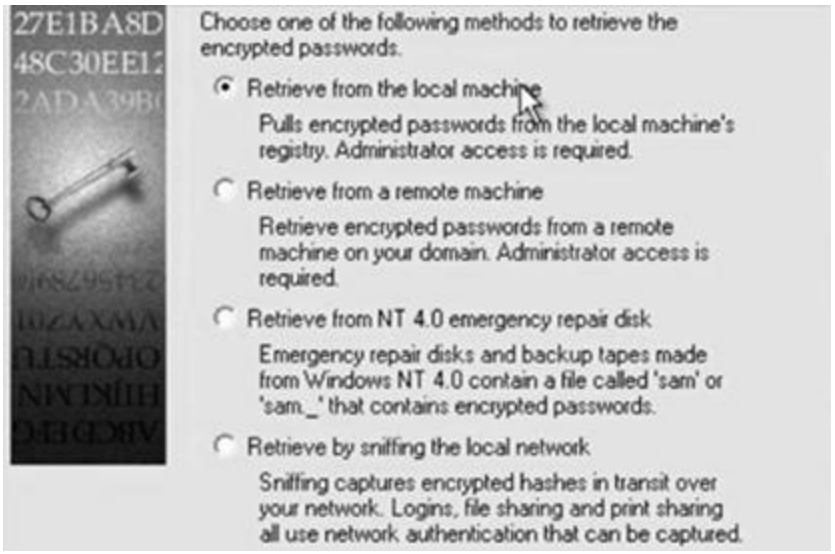
W najbliższych poddziałach czytelnik dowie się kilku ciekawostek na temat systemu Windows oraz najlepszych praktyk związanych z bezpieczeństwem. Wyjaśnią one także niektóre polityki bezpieczeństwa dyktowane przez Default Domain Policy.

17.3.1. Polityka haseł

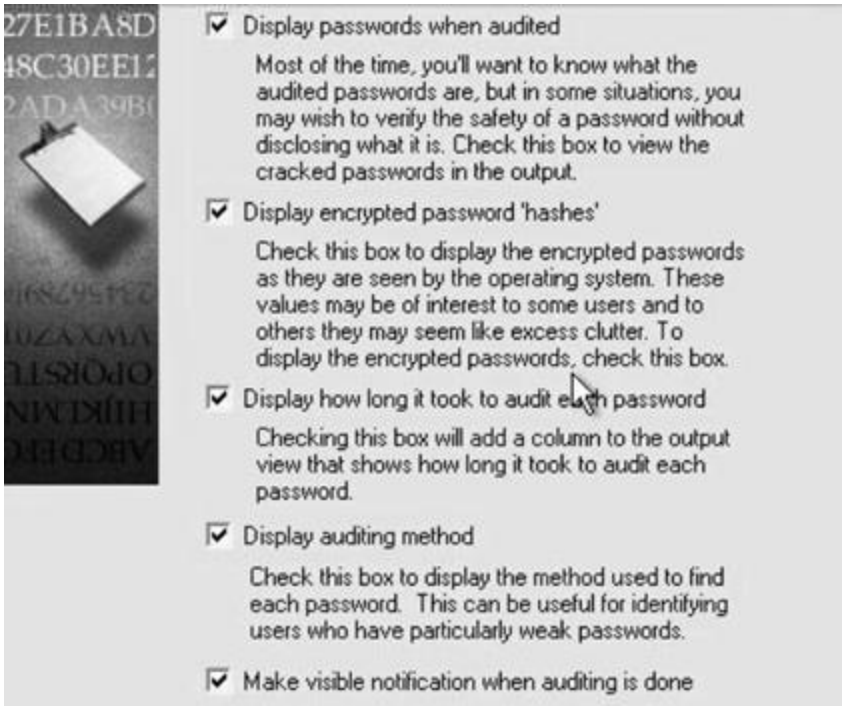
Nadeszła pora na zajęcie się komputerem klienta. W tym momencie, w celach ćwiczeniowych, należy stworzyć dowolnych 4 użytkowników i dać im następujące hasła „a”, „aaa”, „abc”, „kowal”, a także zainstalować program LC5, postępując zgodnie z kreatorem.



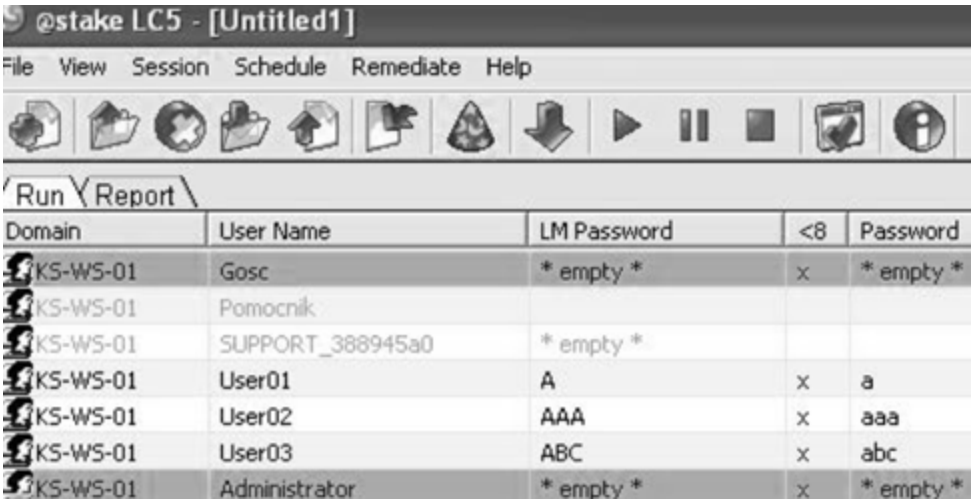
Należy wybrać pierwszą opcję Komputer Lokalny (Retrieve from the local machine).



W przykładzie zostanie wybrana najprostsza metoda łamania haseł.



Resztę ustawień należy zostawić domyślną.



Tak proste hasła zostały złamane w ułamku sekundy najprostszą metodą. Dłuższe hasło „kowal” nie zostało złamane, gdyż nie było go w słowniku. Dlatego tak ważne jest wdrożenie odpowiedniej polityki haseł. Polecić można do przetestowania programy takie jak IRIS do przechwytywania haseł podczas logowania do usług, np. FTP czy Telnet, a także WireShark do podsłuchiwania ruchu w sieci. Dlatego też ważne jest, aby hasła w sieci miały odpowiednią złożoność, a sama komunikacja wewnątrz sieci była jak najlepiej zabezpieczona.

17.3.2. Podmiana logon.scr

Można teraz spróbować nieco podnieść swoje uprawnienia, jeśli ma się dostęp do dysku C. Aby to zrobić, należy.

1. Zalogować się jako administrator, uruchomić program regedit i zmienić wartość klucza: ScreenSaveTimeOut na wartość 15 (sekund) oraz ScreenSaveActive na wartość 1. (HKEY_USERS\.DEFAULT\Control Panel\Desktop).

2. W katalogu %systemroot%\System32 skopiować następujące pliki: logon.scr na logon.old.scr cmd.exe na logon.scr.

3. Wylogować się i odczekać około 15 sekund.

4. Po pojawieniu się konsoli (okna poleceń) wykonać następujące próby (uwaga: niektóre z nich należy powtórzyć kilkakrotnie, ograniczając do niezbędnego minimum ilość otwartych okien):

A. Określić kontekst użytkownika (wykorzystać program whoami z Resource Kit);

B. Uruchomić konsolę lusrmgr.msc i wypróbować możliwości:

- zmiany hasła dla konta administratora,

- utworzenia nowego konta użytkownika,

- zmiany składu grup Administratorów.

C. Po zamknięciu konsoli lusrmgr.msc, uruchomić program explorer.exe i zbadać możliwości wykorzystania Narzędzi administracyjnych (np. wyczyścić plik dziennika systemowego).

D. Zamknąć okno poleceń.

5. Zalogować się jako administrator.

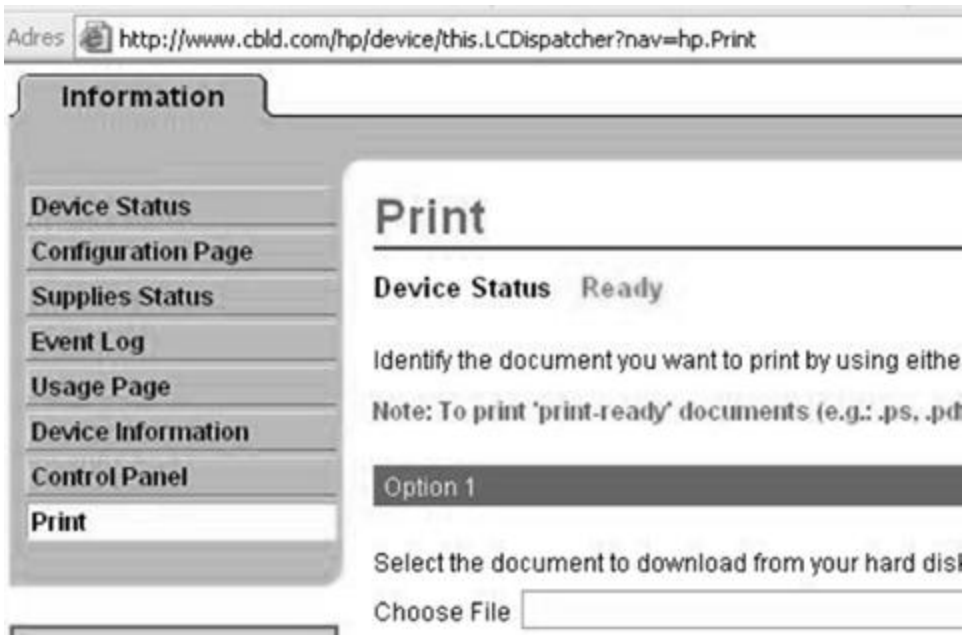
6. Przywrócić pierwotne wartości kluczy w rejestrze, zmienione podczas realizacji punktu 1.

7. Przywrócić pierwotny stan plików zmieniony podczas realizacji punktu 2.

17.3.3. Niezabezpieczone serwery wydruku

Należy teraz wpisać w wyszukiwarce internetowej Google.pl takie zapytanie inurl:hp/device/this.LCDispatcher, jest to adres własny dla serwera wydruku dla drukarek HP.

Często administratorzy nie zabezpieczają serwerów, a dodając stronę do wyszukiwarek automatycznie, Google zapisuje rekord drukarek. Wystarczy wejść w jakiś znaleziony link.



Można teraz zrobić komuś żarcik i coś wydrukować na jego drukarce.

Na koniec strony godne polecenia:

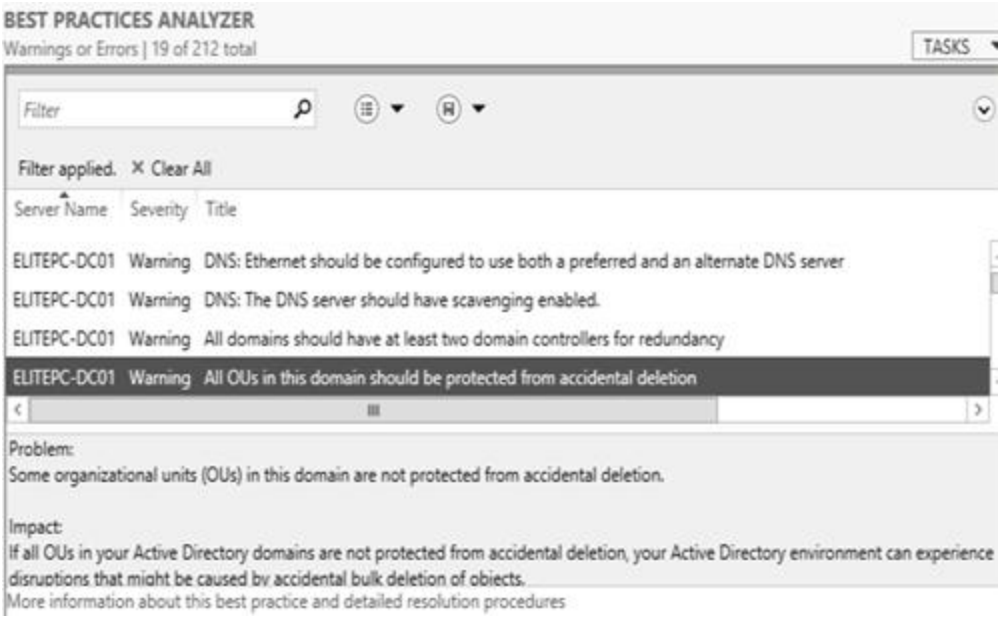
http://www.auditmypc.com/security-scan.asp – gdzie łatwo będzie sprawdzić bezpieczeństwo systemu z zewnątrz:

http://www.backtrack-linux.org/ – gdzie znajduje się Linux naszpikowany programami hakerskimi.

17.3.4. Best Practices Analyzer

Po zainstalowaniu i skonfigurowaniu wszystkich niezbędnych komponentów serwera warto jeszcze użyć narzędzia, które znajduje się w Menadżerze serwera po kliknięciu w Serwer lokalny (Local Server) w lewym menu.

Jest nim okno zarządzania najlepszymi praktykami. Są to wytyczne, uważane za idealny sposób konfiguracji środowiska Windows Server, w normalnych warunkach.



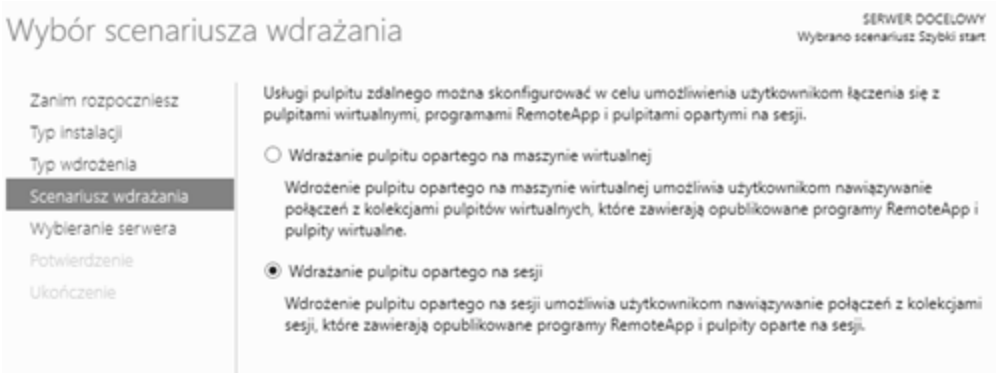
18. Remote Desktop Services

Przed rozpoczęciem instalacji usług terminalowych, jeżeli dokonywane były istotne zmiany w konfiguracji IIS, w ramach tego kursu najrozsądniej będzie odinstalować tę rolę, a następnie przystąpić do instalacji serwera terminali (w Windows 2016 jest to Usługa pulpitu zdalnego [Remote Desktop Services]). Do instalacji tej roli niezbędne są takie składniki, jak: NPS, IIS, Usługi certyfikatów oraz Active Directory. Wdrożenie nie może mieć miejsca na kontrolerze domeny, a komputer musi być przyłączony do domeny.

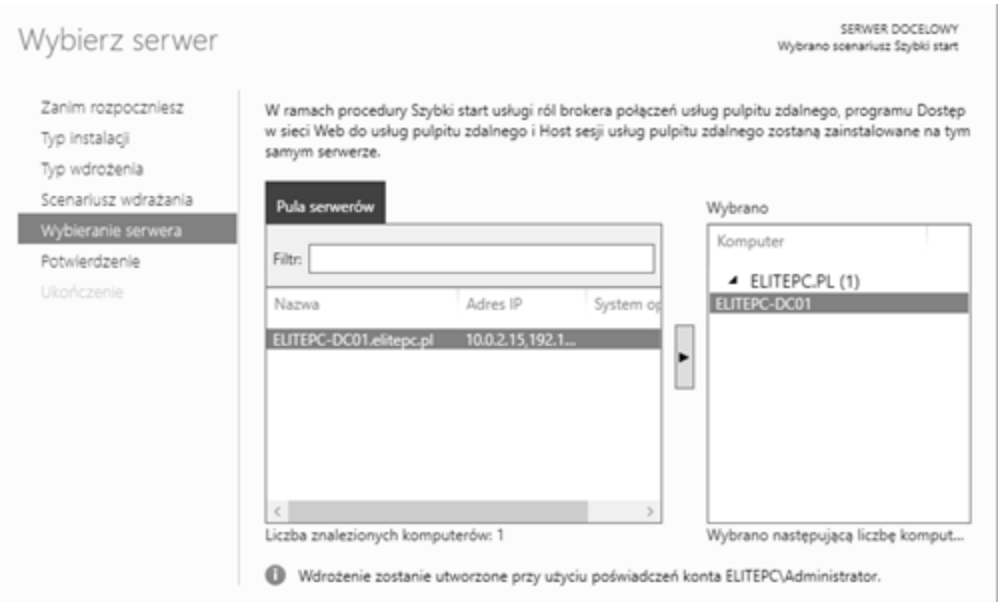
Należy uruchomić kreatora dodawania ról i funkcji serwera. Tym razem nie wybiera się jednak instalacji opartych na rolach lub funkcjach, lecz zaznacza opcję Instalacja Usługi Pulpitu Zdalnego (Remote Desktop Services Installation).

Kolejnym krokiem będzie określenie typu wdrożenia. Do wyboru jest Wdrożenie standardowe (Standard Deployment), które pozwala na instalację na wielu serwerach jednocześnie. W przypadku ćwiczeniowym można zdecydować się na opcję Szybki start (Quick Start), która pozwoli zainstalować szybko i w prosty sposób Usługi pulpitu zdalnego na jednym serwerze, skonfigurować kolekcję i opublikować Zdalne aplikacje (RemoteApp).

W kolejnym oknie kreatora należy zdefiniować scenariusz wdrożenia. Do wyboru są dwie opcje. Wdrożenie oparte na maszynach wirtualnych (Virtual Machine – Based Desktop Deployment) pozwala użytkownikom na łączenie się z przygotowanymi wcześniej maszynami wirtualnymi i korzystanie z zainstalowanych na nich aplikacji. Drugą opcją, która zostanie wybrana w ramach ćwiczenia, jest wdrożenie oparte na sesjach (Session – Based Desktop Deployment), które tak naprawdę jest utożsamiane z usługami terminalowymi. W tym podejściu użytkownicy nie potrzebują maszyn wirtualnych, ponieważ instancje ich aplikacji mogą się być wykonywane niezależnie na jednym serwerze.



W kolejnym kroku określa się serwer, na którym będzie dokonywane wdrożenie.

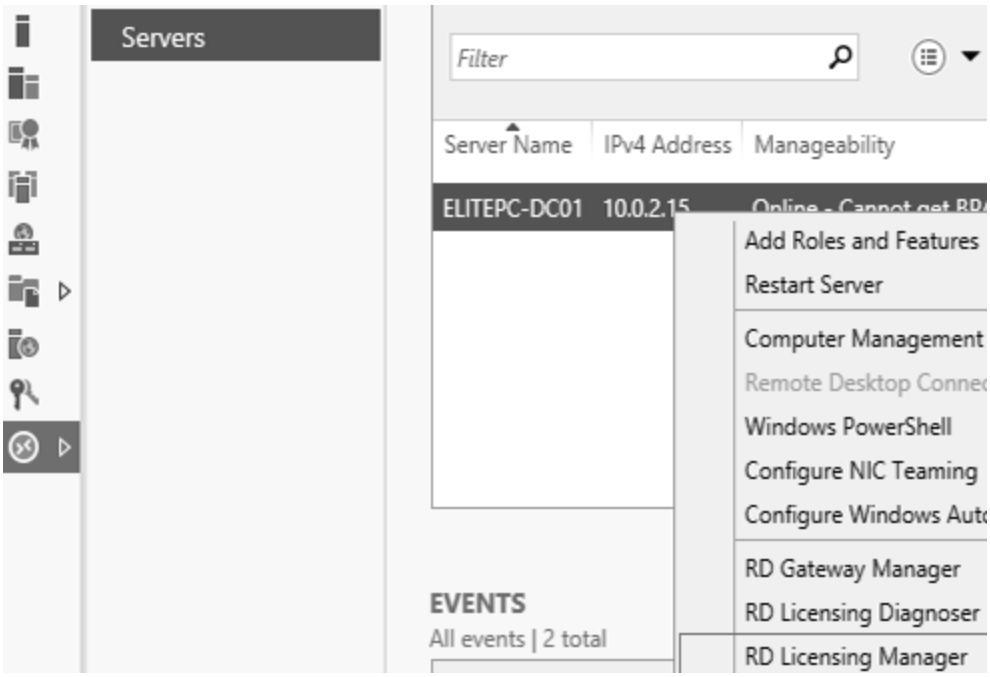


Następnie pojawi się okno podsumowania, gdzie, po zaznaczeniu opcji umożliwiającej automatyczne ponowne uruchamianie serwera, można użyć przycisku Wdroż (Deploy), który rozpocznie cały proces.

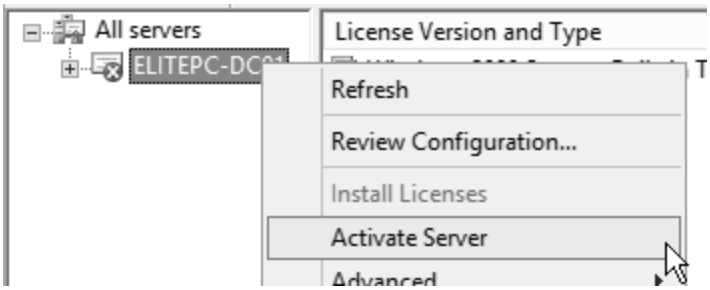
Proces instalacji składa się z trzech etapów: wdrażania usług systemu zdalnego (Remote Desktop Services role services), tworzenia kolekcji sesji (Session collection) oraz uruchamiania programów RemoteApp (RemoteApp programs). Podczas tego procesu komputer kilkakrotnie uruchomi się ponownie.

Po jakimś czasie RDS będą zainstalowane. Należy je jeszcze skonfigurować. Jeżeli nie zostanie wprowadzona żadna licencja (kupuje się je osobno w firmie Microsoft), zyska się 120 dni okresu próbnego. Można ściągnąć teraz z Internetu jakiś program, np. CDBurnerXP, służący do nagrywania płyt CD. Po jego ściągnięciu program należy zainstalować. Ważne jest to, aby aplikację instalować dopiero po zainstalowaniu roli serwera.

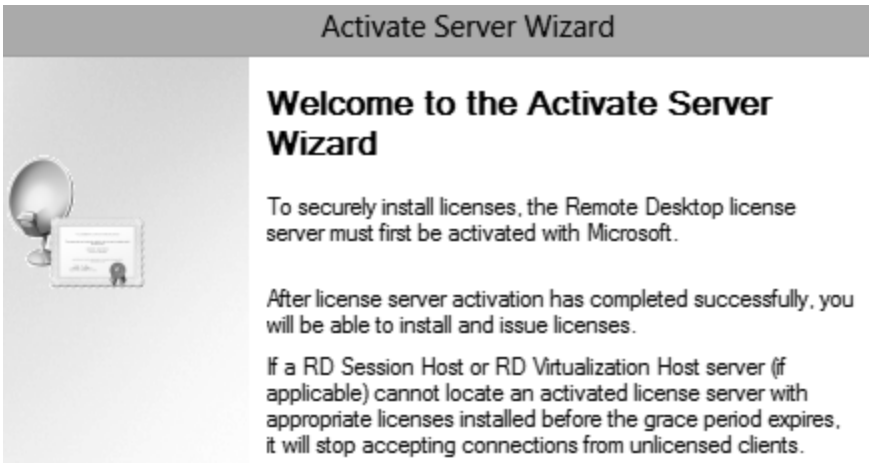
Gdy wgrane są już wszystkie aplikacje, które docelowo będą udostępniane w sieci, warto pomyśleć o konfiguracji licencjonowania serwera terminali. Można jej dokonać z poziomu Menadżera Serwera, rozwijając Remote Desktop Services, następnie wybierając z listy serwerów ten, który jest interesujący i wybierając z menu kontekstowego RD Licensing Manager.



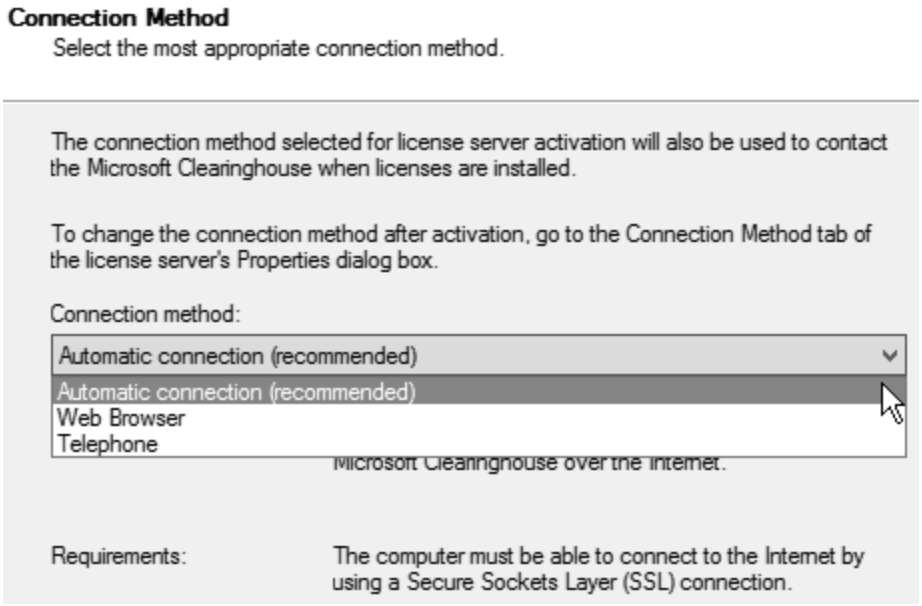
Domyślnie serwer licencjonowania nie jest aktywny. Aby go uaktywnić, klika się w niego prawym przyciskiem myszy i wybiera Aktywuj serwer (Activate Server).



Pierwszym krokiem przed wprowadzeniem licencji jest aktywacja serwera w firmie Microsoft, o czym informuje pierwsza karta kreatora.

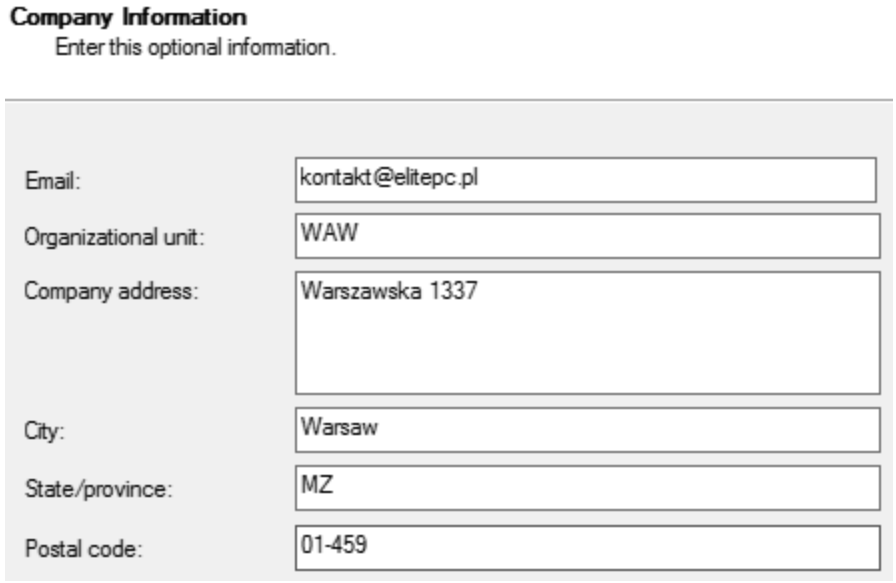


W kolejnym kroku określa się, czy aktywacja ma się odbyć przez Internet, czy telefon, bądź też pozostawia opcje domyślne, czyli wybór automatyczny, który w pierwszej kolejności dokona próby aktywacji przez Internet.



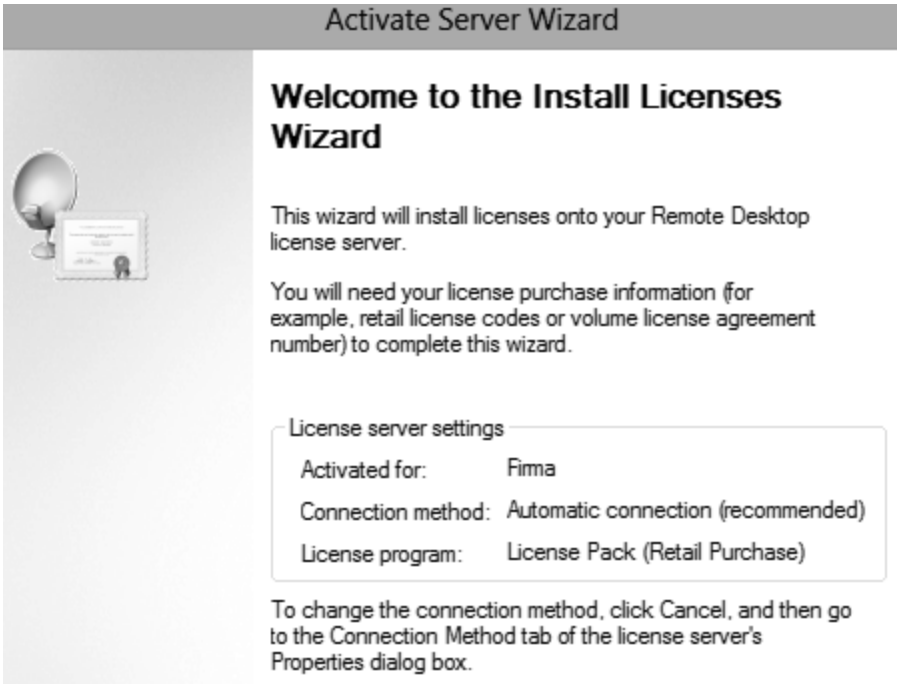
W następnym oknie wypełnia się informacje dotyczące osoby dokonującej aktywacji, firmy oraz kraju pochodzenia.

Kolejna karta stanowi uzupełnienie danych przedsiębiorstwa.

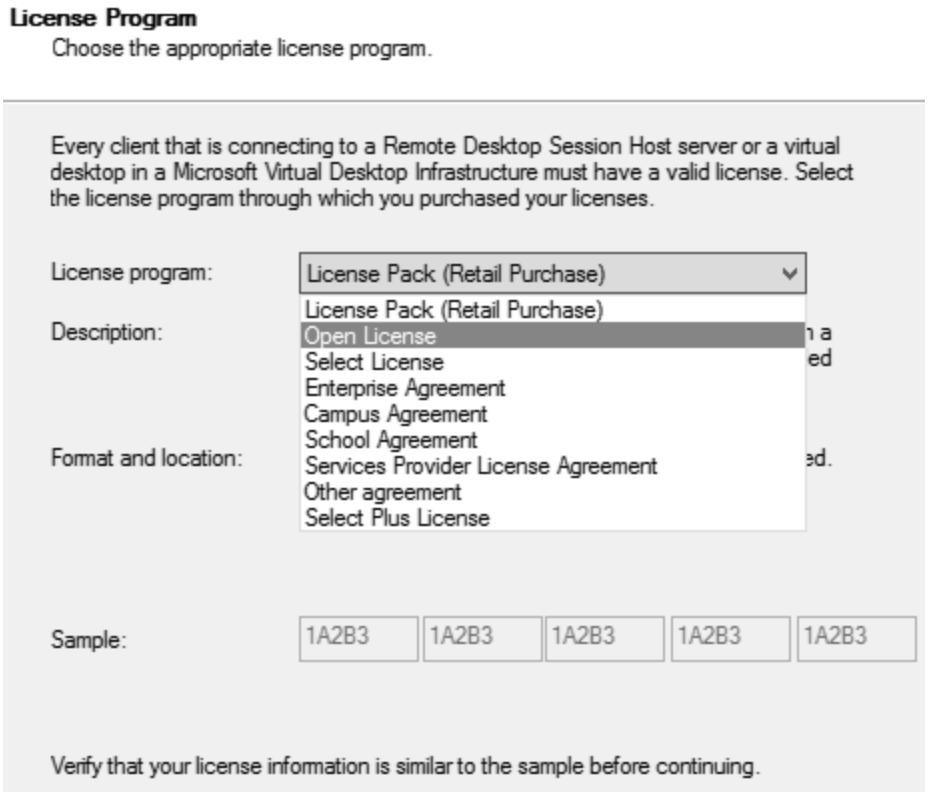


Po kliknięciu w przycisk Dalej (Next) nastąpi aktywacja i wyświetli się karta podsumowująca, gdzie można uruchomić kreatora instalacji licencji poprzez zaznaczenie opcji Rozpocznij kreatora instalacji licencji (Start Install Licenses Wizard Now) i wybranie przycisku Dalej (Next).

Decydując się na tę opcję, pojawi się pierwsze okno nowego kreatora, informujące o jego zadaniu i wymaganiach.

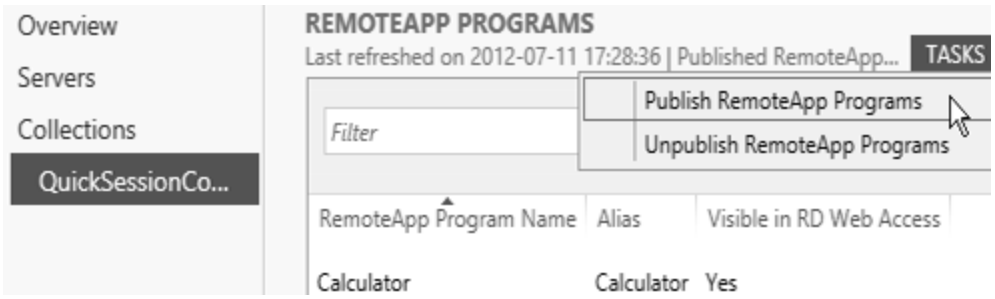


W kolejnym oknie wybiera się obejmujący firmę program licencjonowania i podaje na kolejnych kartach niezbędne dane.

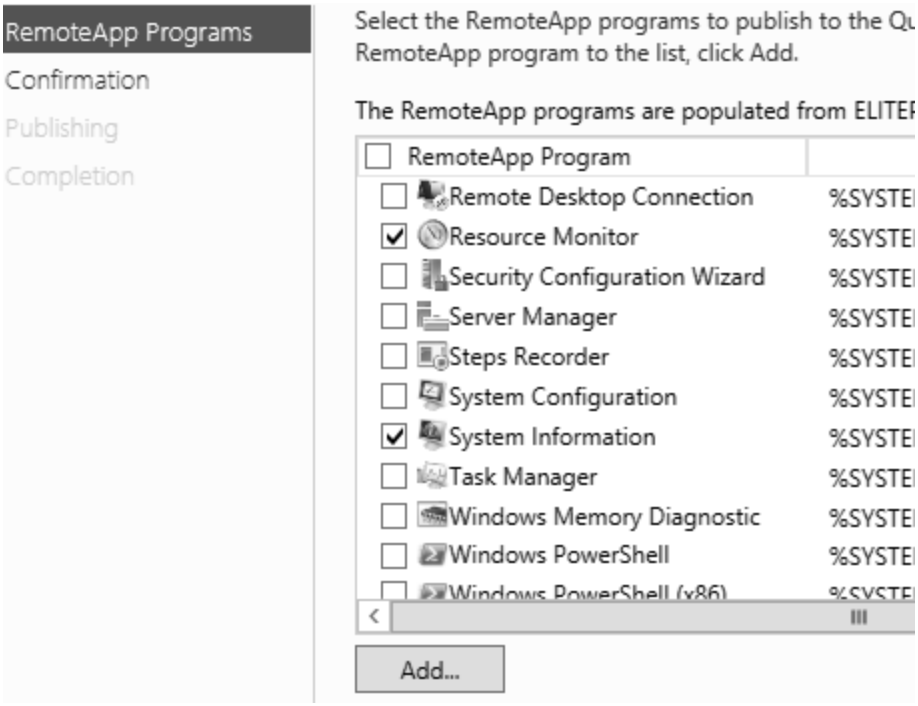


Jeżeli ten krok zostanie pominięty, uzyska się 120 dni okresu próbnego.

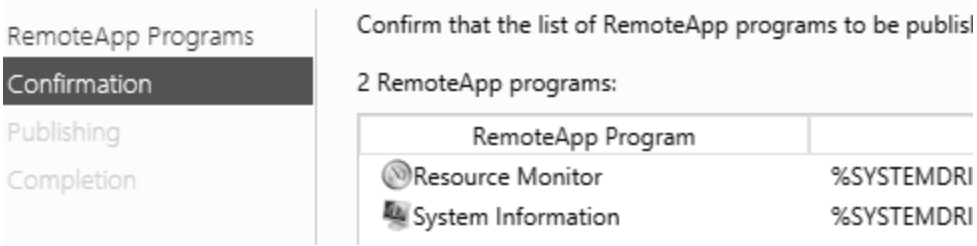
Na serwerze, na którym został zainstalowany RDS po uruchomieniu Menadżera serwera, rozwinięciu Usługi pulpitu zdalnego (Remote Desktop Services) z menu po lewej stronie, następnie Kolekcji (Collections), a potem Kolekcji szybkiej sesji (Quick Session Collection), można znaleźć kolekcję utworzoną przez kreatora w czasie instalacji. W sekcji Zdalne aplikacje (RemoteApp Programs) za pomocą przycisku Zadania (Tasks) wybiera się opcję Opublikuj zdalne aplikacje (Publish RemoteApp Programs) w celu udostępniania programów w trybie RemoteApp. Standardowo udostępniony jest Kalkulator, Paint oraz Wordpad.



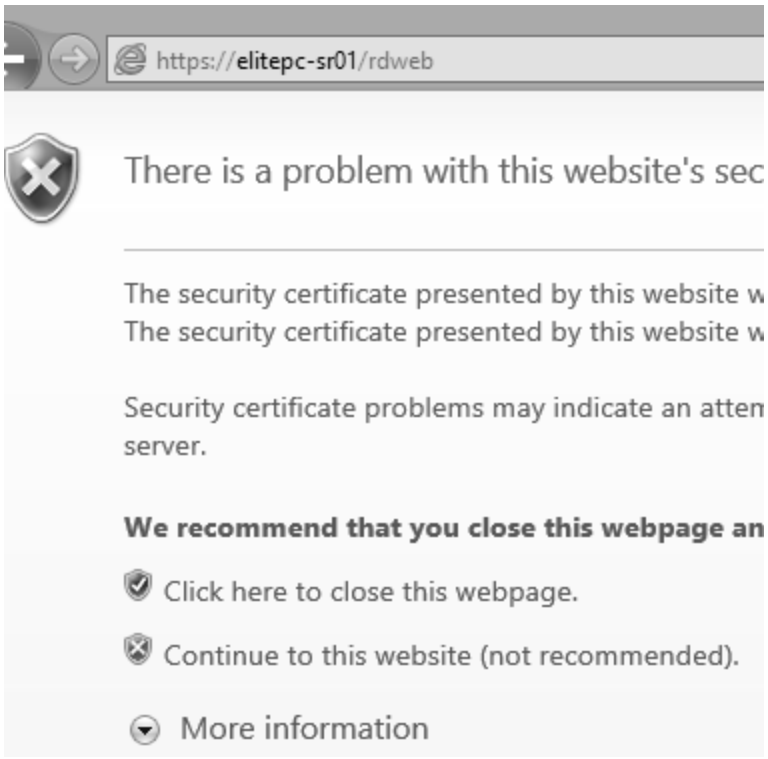
Pojawi się kreator, w którym należy zaznaczyć aplikacje, mające zostać udostępnione, lub przyciskiem Dodaj (Add) dodaje się aplikacje, których nie ma na liście.



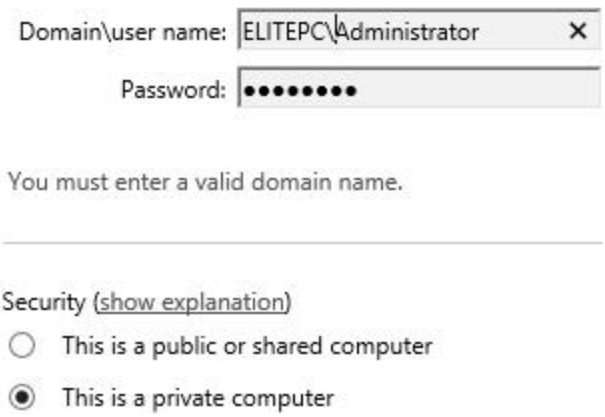
Pojawi się karta podsumowująca, w której należy kliknąć przycisk Publikuj (Publish), a po chwili przycisk Zamknij (Close).



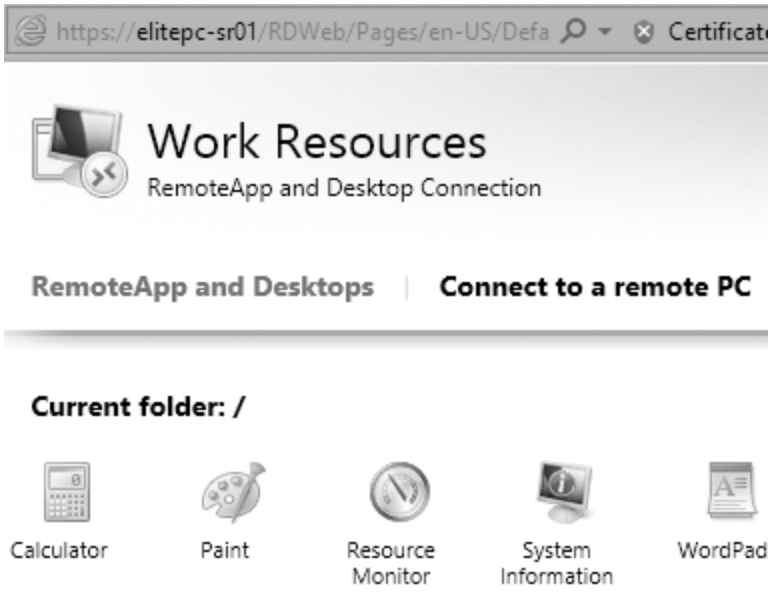
Po wpisaniu w przeglądarce adresu https://adres_serwera.pl/RDWeb/ nastąpi przeniesienie na stronę, która oferuje możliwość uruchomienia wcześniej udostępnionych aplikacji, jak również dostępu za pomocą terminali do komputerów wewnątrz sieci. Ważnym aspektem tych działań jest to, że aplikacje uruchamiane w ten sposób działają w kontekście serwera, czyli nie obciążają komputerów klienckich.



W przypadku braku certyfikatu z podpisem cyfrowym konieczne będzie zaakceptowanie wyjątku bezpieczeństwa. Kiedy zostanie potwierdzony, pojawi się ekran logowania, gdzie należy podać hasło użytkownika oraz jego nazwę poprzedzoną nazwą domeny. Określa się także, czy komputer wpięty jest do bezpiecznej sieci prywatnej, czy publicznej.



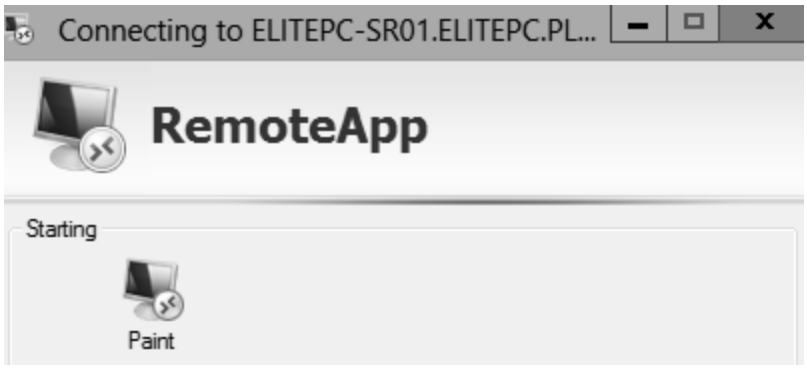
Po wejściu do zakładki Zdalne aplikacje i pulpity (RemoteApps and Desktops) można znaleźć aplikacje udostępnione na serwerze, zarówno dostępne w samym systemie, jak i dodatkowo zainstalowane, w tym ściągnięty z internetu CD Burner XP.



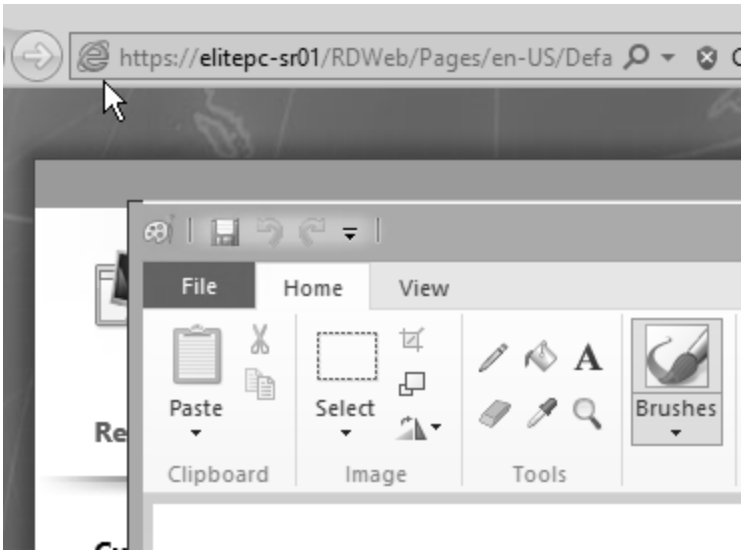
Aby uruchomić jakąś aplikację, wystarczy kliknąć na niej myszką.

Pojawi się ekran przypominający połączenie pulpitu zdalnego, na którym, zostawiając opcje domyślne, należy kliknąć w przycisk Połącz (Connect).

Rozpocznie się nawiązywanie połączenia z serwerem, które może potrwać kilka chwil.



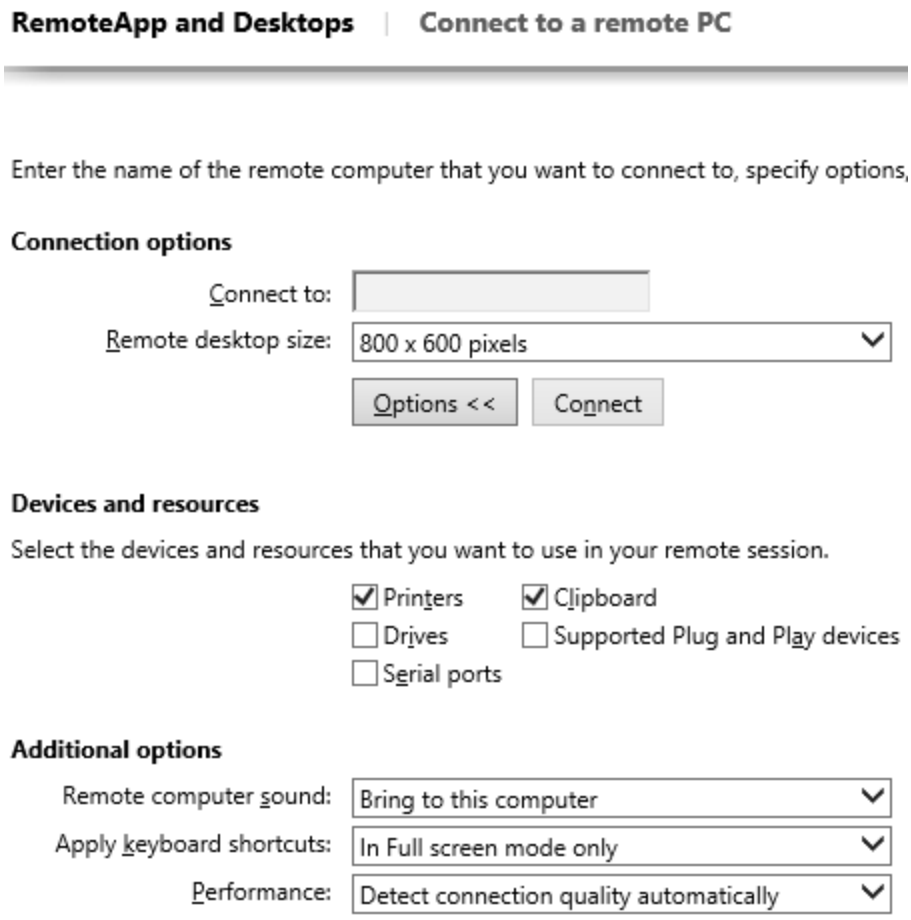
Gdy aplikacja zostanie uruchomiona, mimo że działa ona w kontekście serwera, na systemie klienckim nie widać różnicy w działaniu aplikacji, jak gdyby była ona zainstalowana na komputerze klienckim.



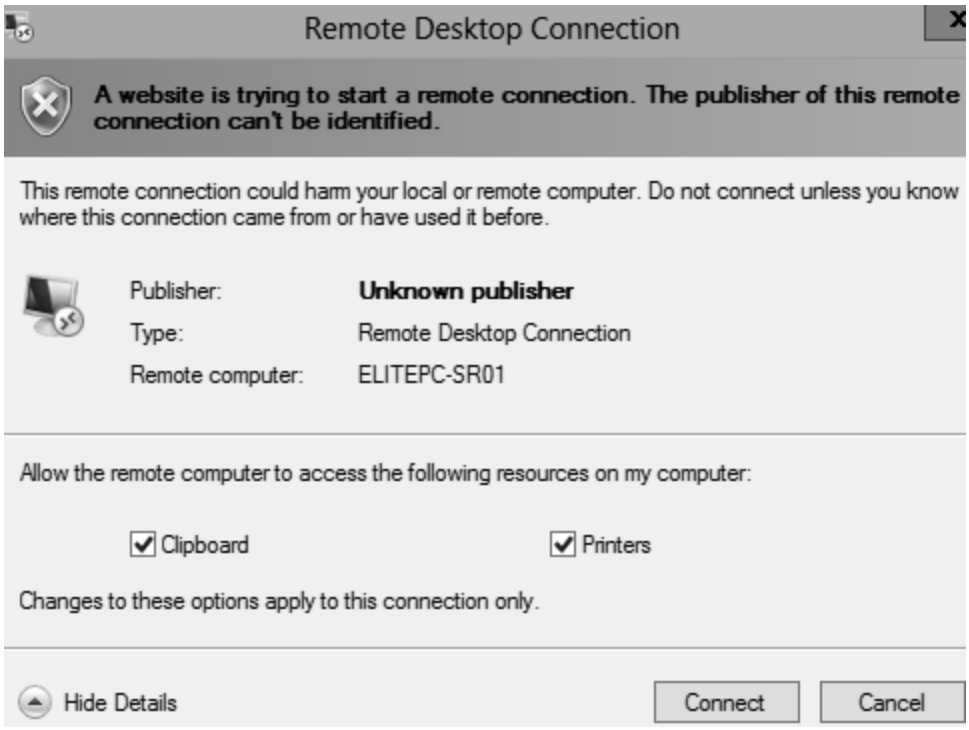
Aplikację uruchomioną w trybie RemoteApp rozpoznać można na pasku Start poprzez znaczek symbolizujący połączenie zdalne, narzucony na ikonę programu.

Po wejściu w zakładkę Połącz się ze zdalnym komputerem (Connect to a Remote PC) można podłączyć się do

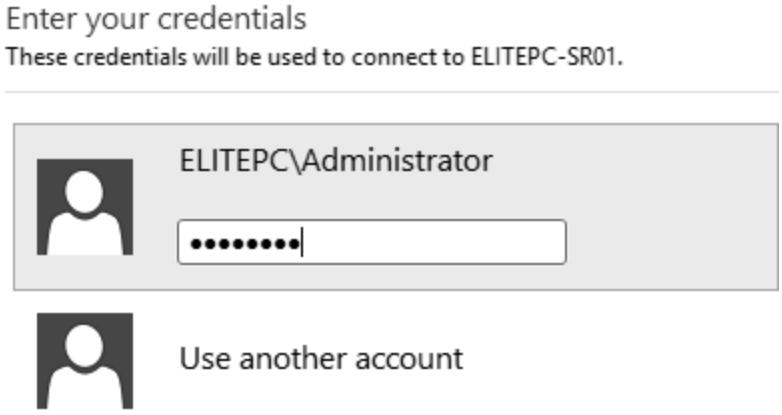
komputera znajdującego się w sieci firmowej poprzez połączenie pulpitu zdalnego; można też określić rozdzielczość okienka, w którym ma być nawiązane połączenie, oraz uruchomić inne opcje znane już z nawiązywania tradycyjnego połączenia pulpitu zdalnego. Aby się połączyć, wystarczy podać adres serwera oraz użyć przycisku Połącz (Connect).



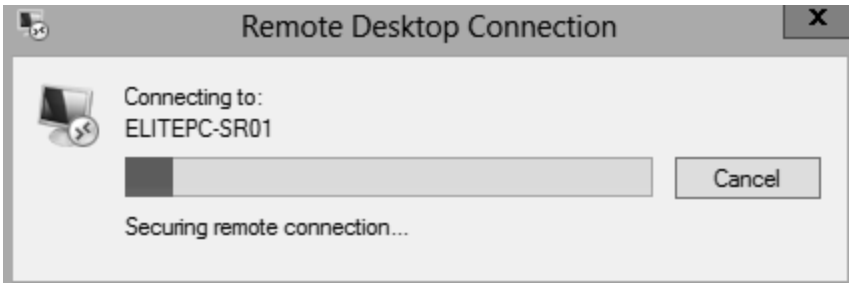
Pojawi się okno połączenia pulpitu zdalnego, w którym należy nacisnąć przycisk Połącz (Connect).



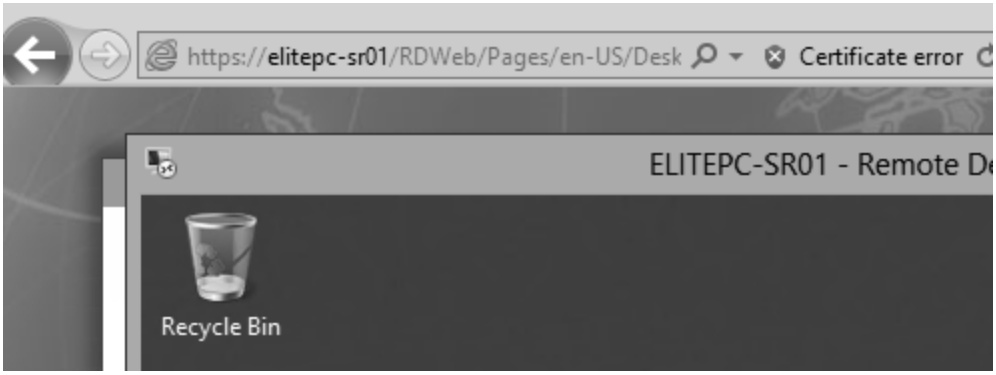
Należy podać dane do logowania, które mają zostać użyte do nawiązania połączenia z komputerem zdalnym.



Nastąpi przygotowywanie i nawiązywanie połączenia zdalnego, które musi zostać zabezpieczone, dlatego też proces ten może chwilę potrwać.

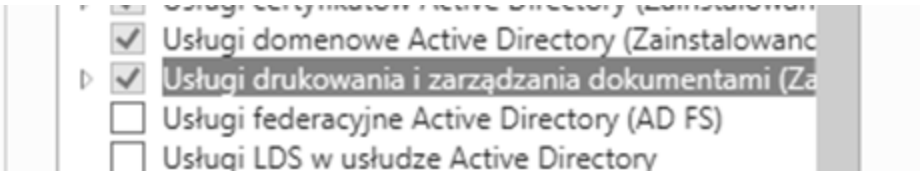


Jeżeli zostało wybrane połączenie pulpitu zdalnego w trybie pełnoekranowym, praca zdalna będzie wyglądać analogicznie do tej znanej z pracy ze zwykłym połączeniem pulpitu zdalnego. W przeciwnym razie, gdy będzie wybrana mniejsza rozdzielczość, zostanie otworzone okienko w tym rozmiarze, a obraz pulpitu komputera zdalnego dostosowany do jego wymiarów.

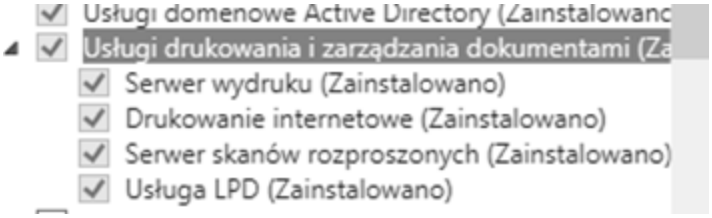


19. Serwer Wydruku

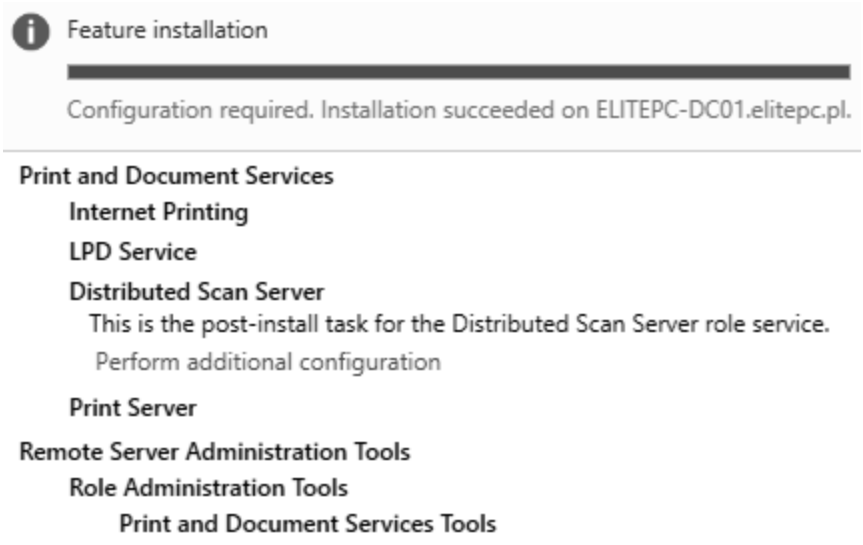
Na początku należy dodać nową rolę do serwera, wybierając z listy Usługi drukowania i zarządzania dokumentami (Print and Document Services). Potem należy kliknąć Dalej (Next).



Należy wybrać wszystkie usługi i kliknąć Dalej (Next).

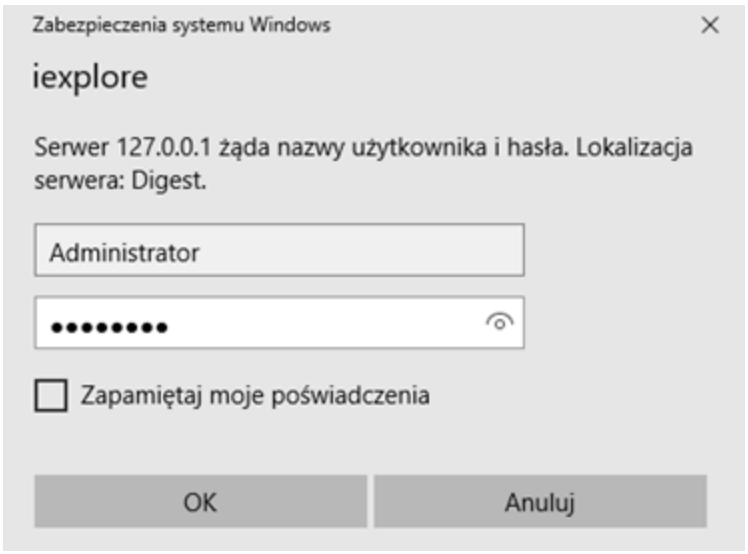


Po wgraniu niezbędnych plików, powinno się ponownie uruchomić komputer, szczególnie jeżeli dodatkowo była instalowana rola IIS.

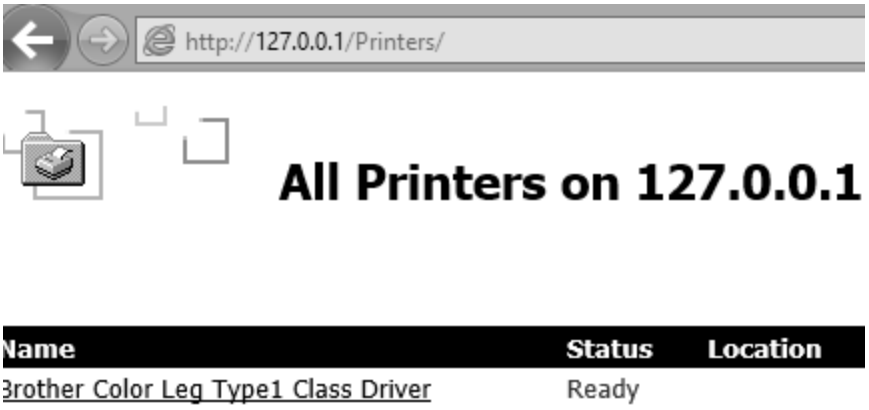


Po wpisaniu adresu http://127.0.0.1/Printers można wejść na stronę, na której zarządza się wydrukami.

System Windows poprosi użytkownika o uwierzytelnienie przed udzieleniem mu dostępu do serwera wydruków.

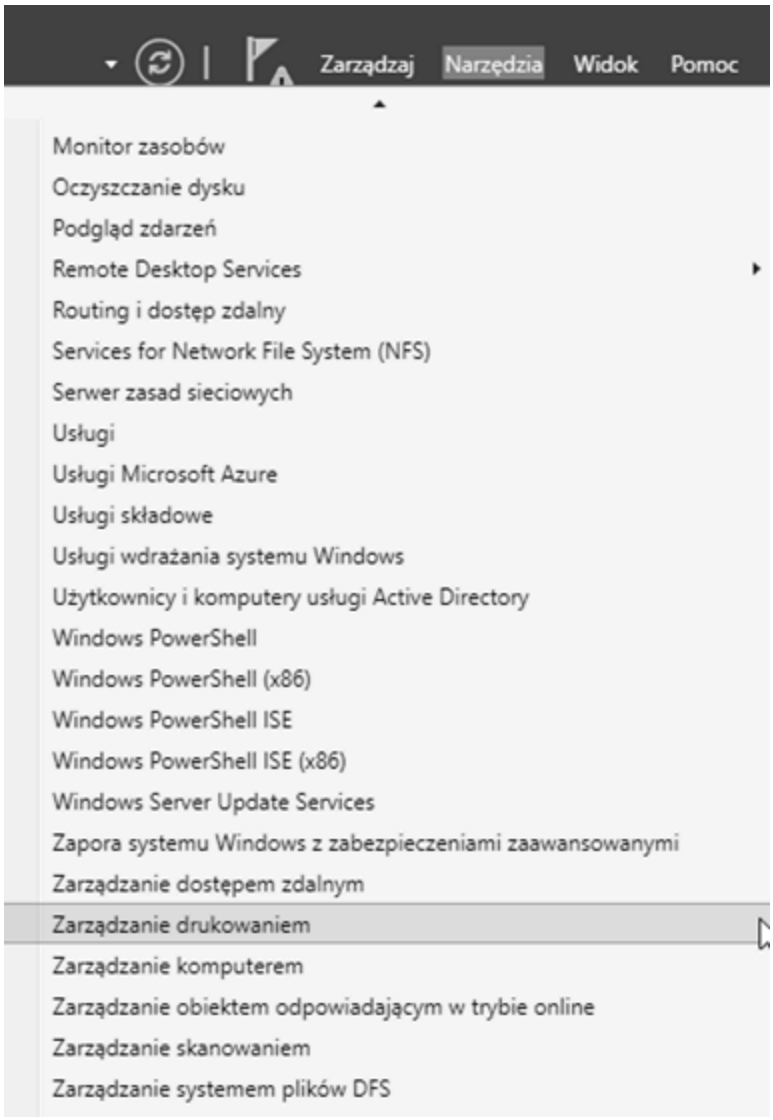


Jeżeli wszystko przebiegnie pomyślnie, użytkownik otrzyma dostęp do udostępnionych drukarek.



Po wybraniu dowolnej z nich, strona www przeniesie użytkownika do podstrony drukarki, na której można nią zarządzać.

Opcje serwera wydruku można skonfigurować, wchodząc do Menadżera serwera i wybierając Narzędzia (Tools), a następnie Zarządzanie Wydrukami (Print Management).

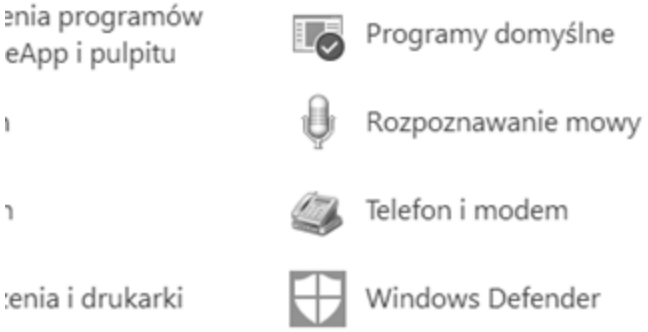


20. Serwer faksów

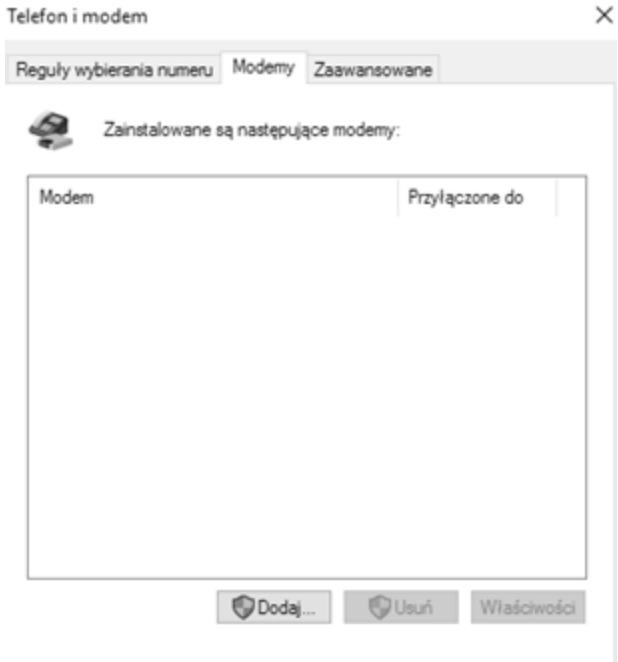
W tym rozdziale zostanie omówiona konfiguracja serwera faksów. Przydatna będzie drukarka. Dla ćwiczeń zostanie zainstalowana wirtualna drukarka, która zapisuje wydruki w formacie PDF, np. BullZIP PDF Printer.

Drugim niezbędnym urządzeniem jest sam modem. Aby serwer działał, potrzebny jest fizycznie zainstalowany modem, podpięty do linii telefonicznej.

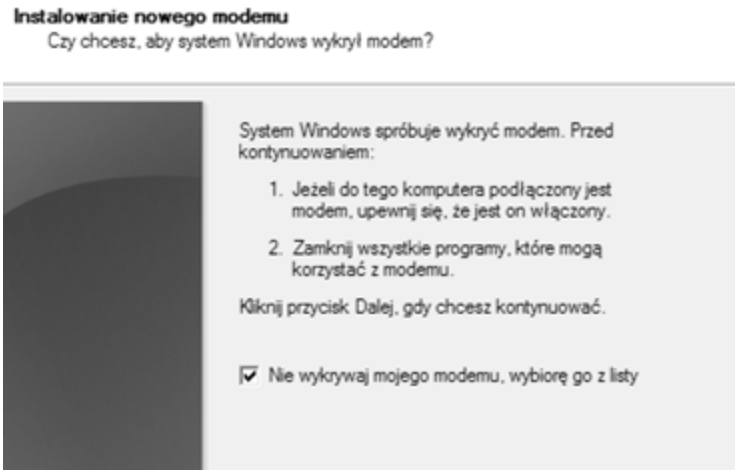
W ten sposób można oszukać system, wymuszając na nim instalację modemu, który nie jest podpięty fizycznie. W panelu sterowania wybiera się opcję Telefon i modem (Phone and Modem).



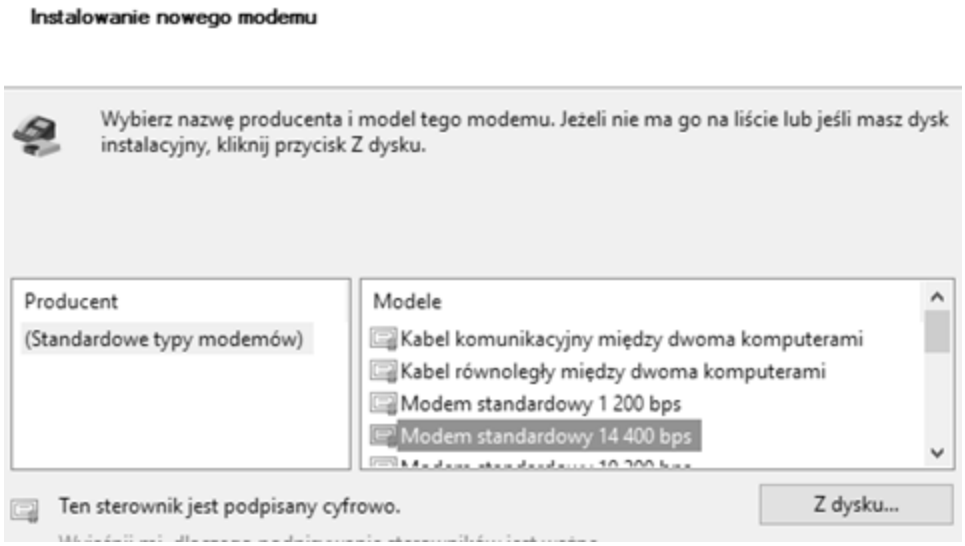
Następnie w zakładce Modem należy kliknąć Dodaj (Add).



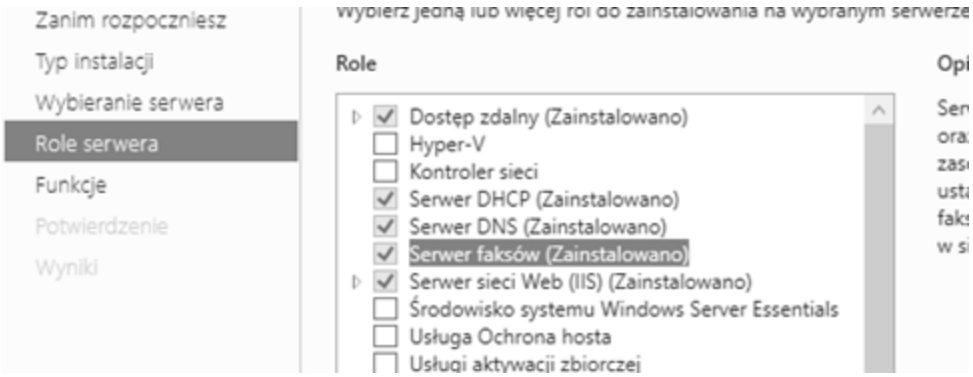
Należy zaznaczyć Nie wykrywaj mojego modemu (Don’t detect my modem: I will select it from a list) i kliknąć Dalej (Next).



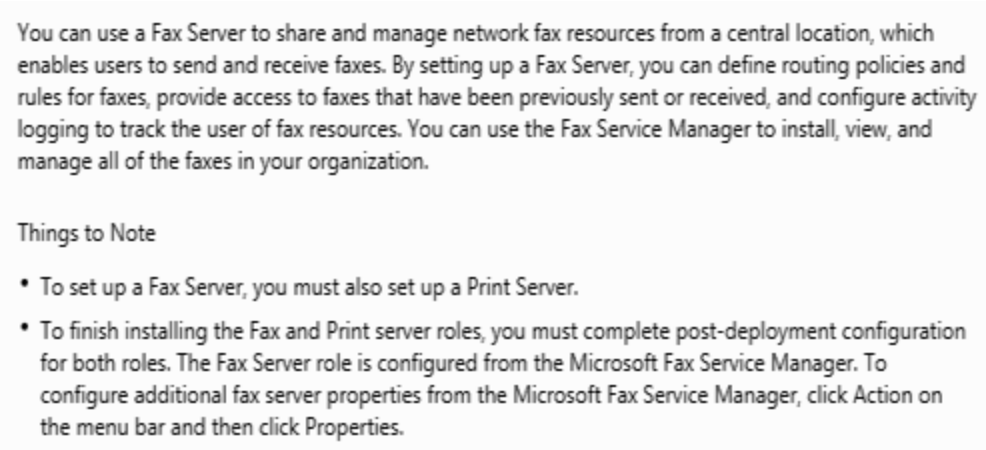
Należy chwilę zaczekać, aż lista się wygeneruje, a następnie wybrać modem z listy.



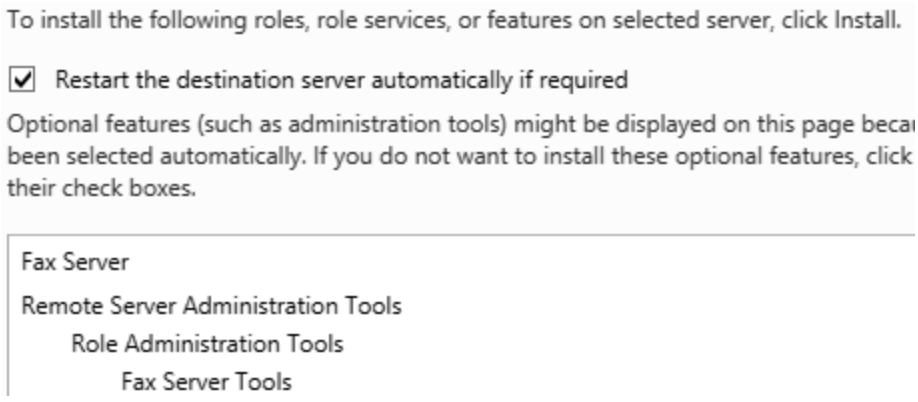
Gdy na komputerze zainstalowane są wszelkie niezbędne urządzenia, można przystąpić do właściwej instalacji serwera wydruku. Należy wybrać i zainstalować rolę Serwer faksów.



Następnie należy kliknąć Dalej (Next).



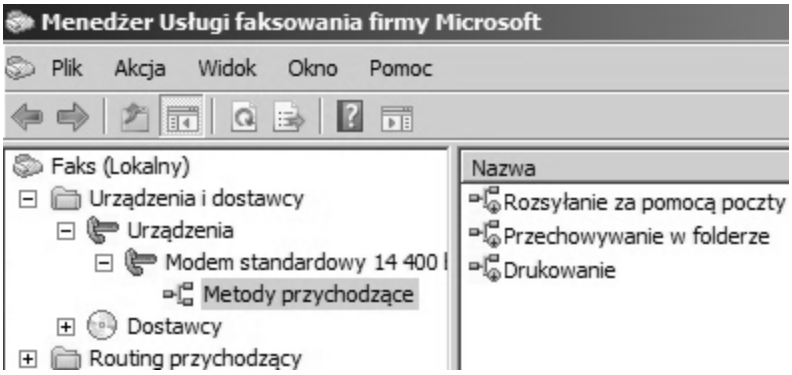
Później trzeba zaznaczyć opcję Uruchom ponownie serwer docelowy, jeśli wymagane (Restart the destination server automatically if required) i kliknąć w przycisk Instaluj (Install).



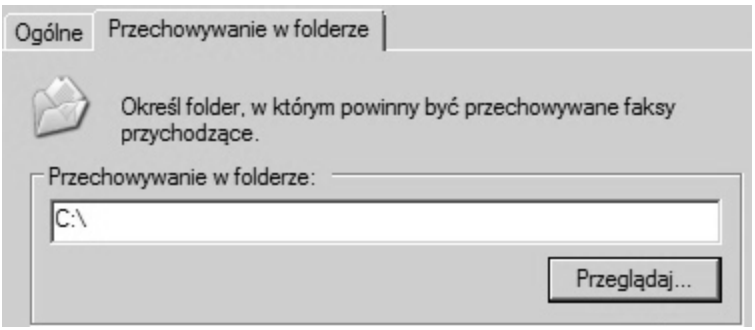
Aby przystąpić do wstępnej konfiguracji serwera, należy wybrać Menadżer Usług Faksowania (Fax Service Manager).

Konsola ta jest identyczna jak w systemie Windows Server 2008 R2.

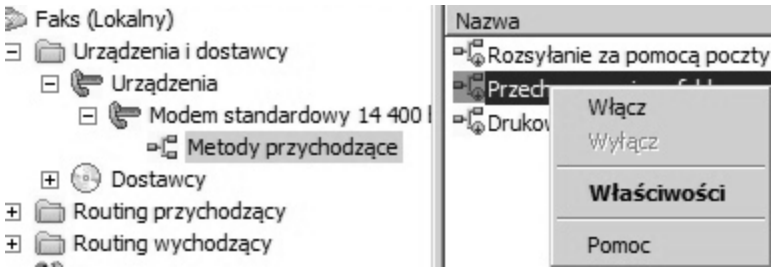
W dalszej kolejności, rozwinąwszy drzewko menu zgodnie z obrazkiem poniżej, można znaleźć trzy metody odbierania faksów. Pierwsza z nich przekaże fax na podany adres email, ostatnia spowoduje wydruk na drukarce, a środkowa zapisze wiadomość w formie pliku. W ćwiczeniu wybrano właśnie tę opcję.



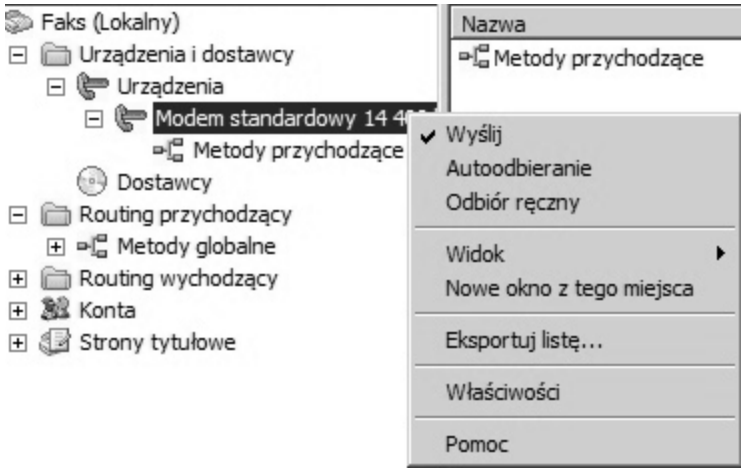
W zakładce Przechowywanie w folderze należy wskazać ścieżkę do folderu, w którym mają być zapisywane pliki i kliknąć OK.



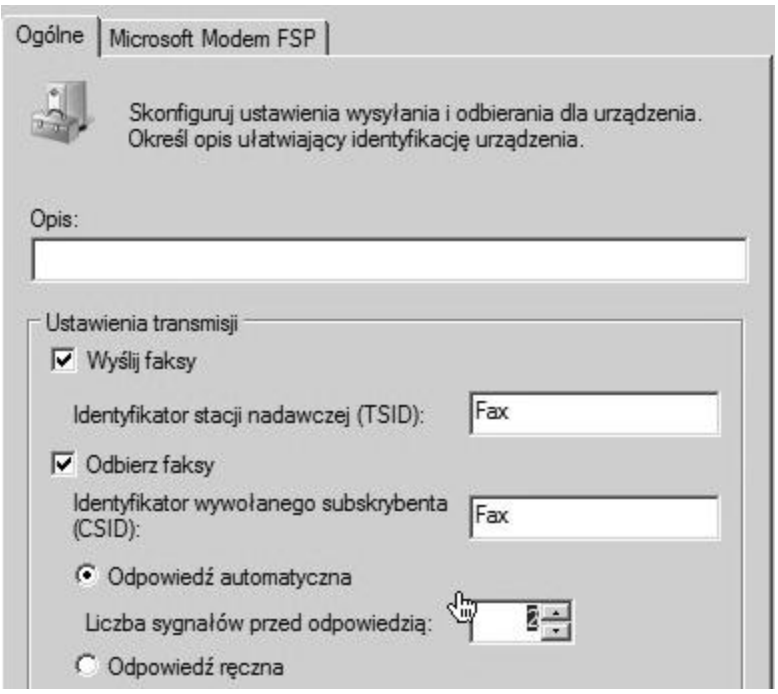
Należy pamiętać, aby użytkownicy wcześniej zdefiniowani mieli dostęp do tego folderu czy też do drukarki, która byłaby konfigurowana. Na koniec należy kliknąć prawym przyciskiem myszy na wybranej opcji i kliknąć Włącz (Enable).



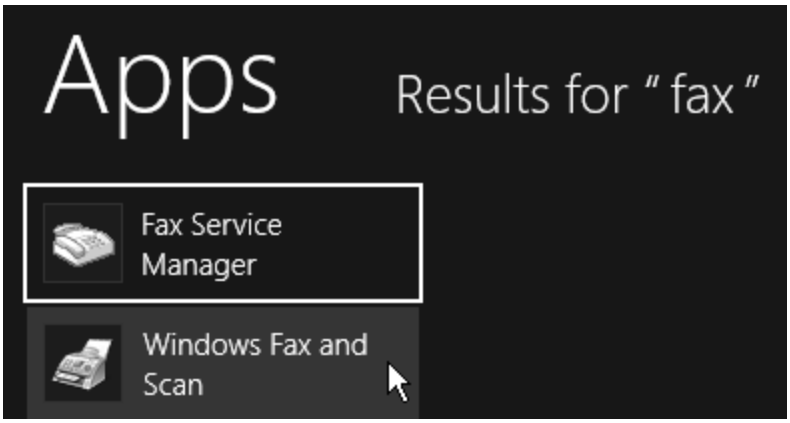
W następnym kroku konieczne jest kliknięcie w modem i wejście w jego Właściwości (Properties).



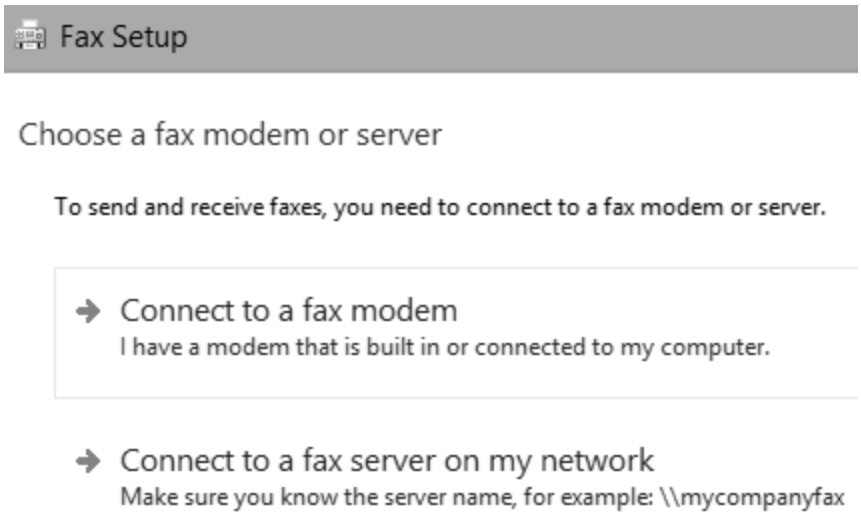
Na karcie Ogólne należy zaznaczyć opcję Odbierz faksy, a następnie ustawić liczbę sygnałów, po jakich faks zostanie odebrany, np. 2.



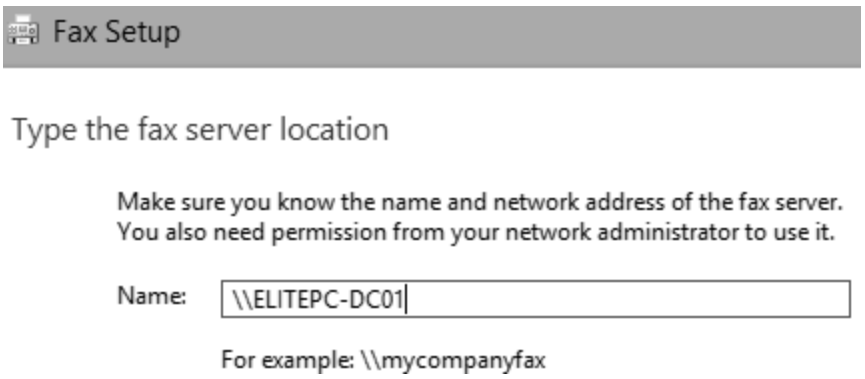
Odbieranie faksów jest już zapewnione, a co z wysyłaniem? Należy kliknąć START i uruchomić Faksowanie i skanowanie w systemie Windows (Windows Fax and Scan).



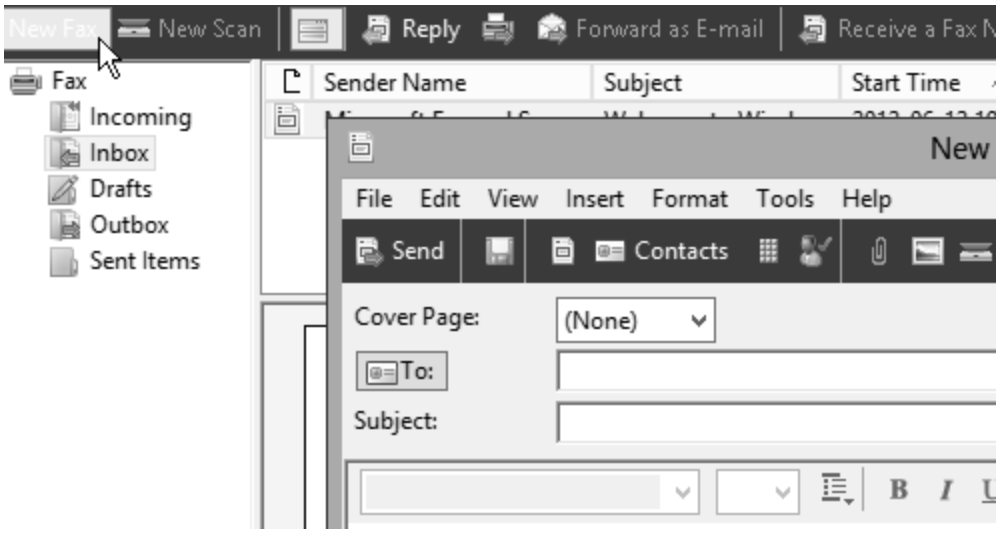
Na ekranie, jaki się pojawi, należy wybrać Połącz z serwerem faksów w mojej sieci (Connect to a fax server on my network).



Następnie należy wpisać nazwę serwera i kliknąć Dalej (Next).



Za pomocą tej aplikacji można tworzyć dokumenty, które będą wysłane za pośrednictwem faksu.



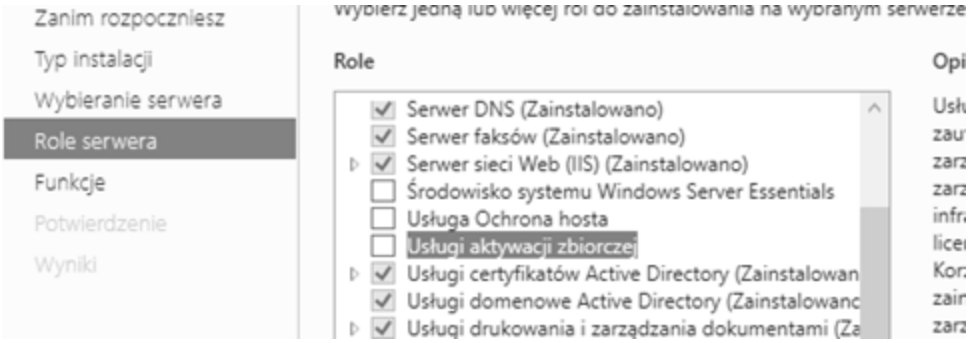
Należy także pamiętać, aby każdy użytkownik, który ma mieć dostęp do usług faksowania, został dodany do grupy Użytkownicy faksu (Fax Users).

21. Volume Activation Services

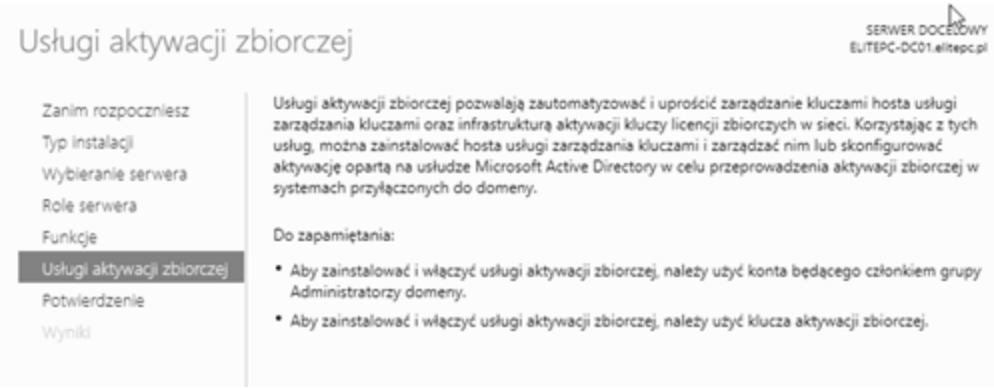
Volume Activation Services jest rolą, która zastąpiła Key Management Service (KMS). Daje ona możliwość aktywacji systemów klienckich, serwerowych oraz innych aplikacji firmy Microsoft w obrębie przedsiębiorstwa bez konieczności nawiązywania bezpośredniego połączenia z serwerami aktywacyjnymi firmy Microsoft. Niniejszy rozdział omawia proces instalacji oraz jej wstępnej konfiguracji.

21.1. Instalacja

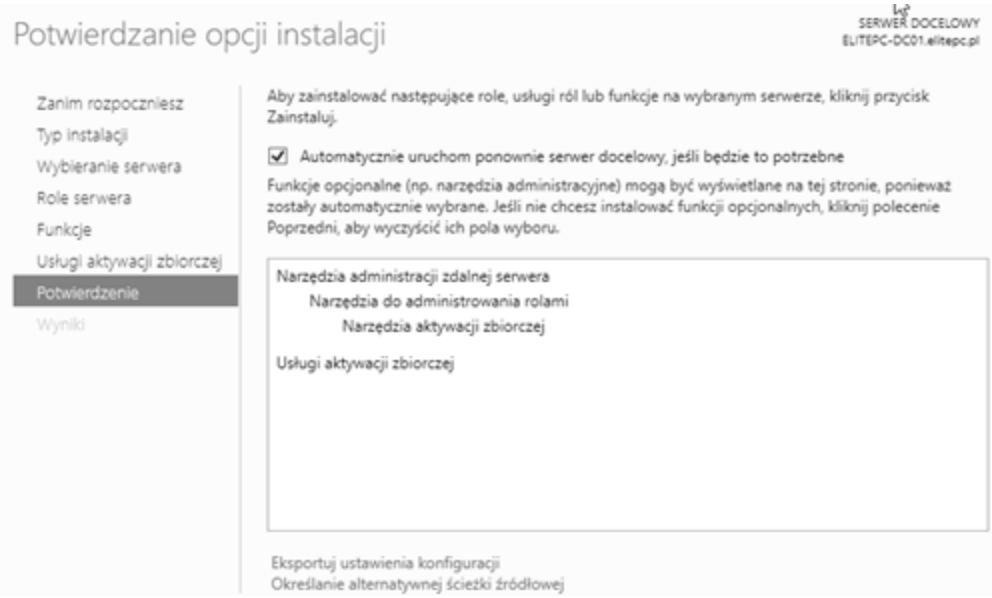
Aby użytkownik mógł zainstalować Volume Activation Services, musi posiadać uprawnienia administratora lokalnego do komputera docelowego oraz być członkiem grupy zabezpieczeń Administratorzy Przedsiębiorstwa (Enterprise Administrators). Instalacji dokonuje się poprzez Menadżera Serwera, używając kreatora dodawania ról i funkcji.



Na pierwszej karcie kreatora instalacji Volume Activation Services pojawiają się informacje o tym, za co ta rola odpowiada oraz jakie są wymagania do jej instalacji. Między innymi można się tutaj dowiedzieć, że niezbędny będzie klucz aktywacji woluminowej.

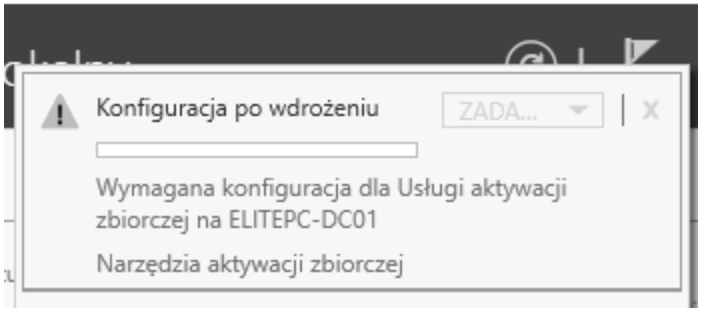


Bezpośrednio po użyciu przycisku Dalej (Next) zostanie wczytana karta podsumowująca, gdzie, w celu zainstalowania roli, należy wybrać przycisk Instaluj (Install).



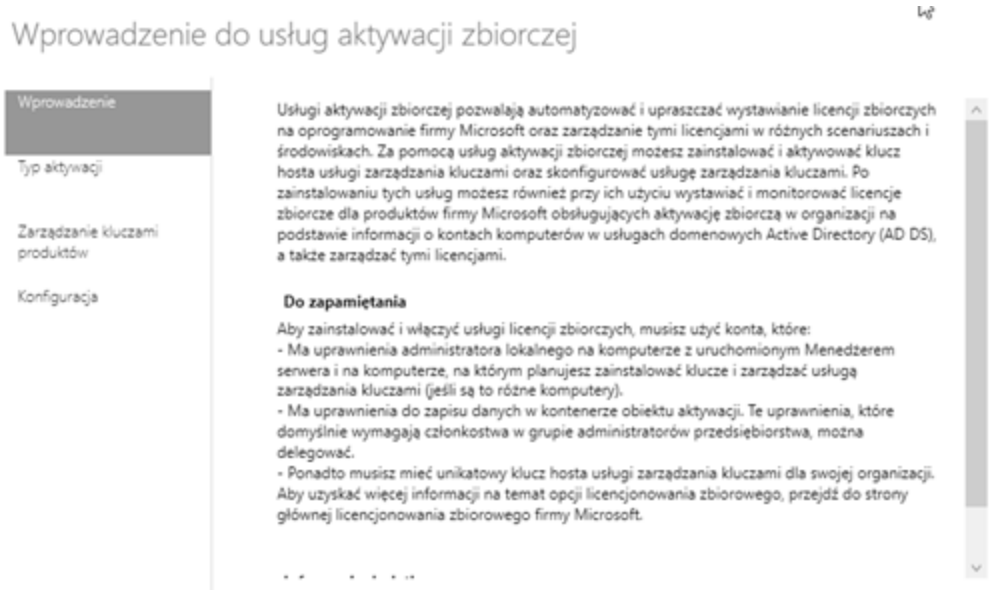
21.2. Wstępna konfiguracja VA Services

W Menadżerze serwera, w menu po lewej stronie, pojawi się rola VA Services. Nie jest jednak ona jeszcze uruchomiona, niezbędna będzie wstępna konfiguracja serwera. Można tego dokonać poprzez Centrum akcji, gdzie klika się w nośnik Volume Activation Tools w sekcji Post-deployment Configuration.

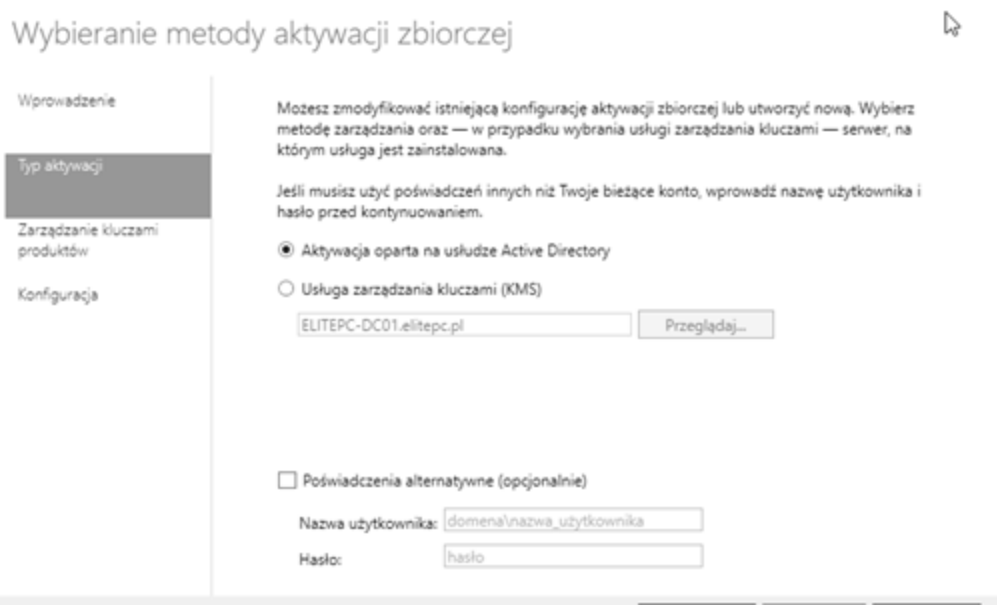


Pojawi się kreator, który składa się z czterech kroków. Pierwszym z nich jest wprowadzenie do usługi. Znajdują się

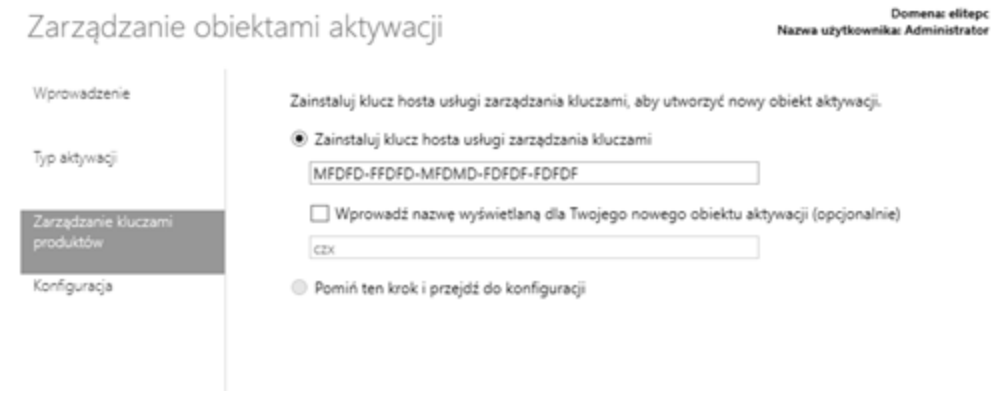
tam informacje na temat samej roli oraz wymagań, jakie muszą zostać spełnione przed dalszą konfiguracją.



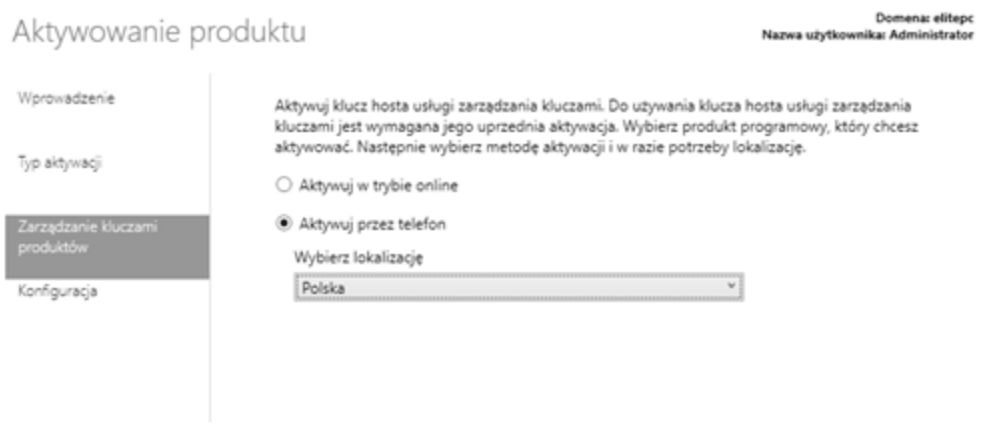
W kolejnym kroku należy określić metodę aktywacji. W przypadku domeny najwygodniej będzie wybrać Autentykacja oparta na Active Directory (Active Directory – Based Activation). Dzięki temu nowa rola dostosuje się do infrastruktury AD i nie będzie wymagana żadna dodatkowa konfiguracja, np. Firewalla. W tym oknie istnieje też możliwość podania nazwy użytkownika i hasła, gdyby obecnie zalogowany na komputerze użytkownik nie miał odpowiednich uprawnień do przeprowadzenia instalacji.



Na kolejnej karcie konieczne jest wprowadzenie numeru licencji klienta, na podstawie której dokonywane będą aktywacje.



Niezbędne będzie połączenie z serwerami Microsoft w celu weryfikacji i aktywacji tego klucza, podobnie jak w przypadku systemów operacyjnych można tego dokonać online lub telefonicznie, zatwierdzając swój wybór przyciskiem Wykonaj (Commit).



Pojawi się komunikat informujący o tym, że do Active Directory zostanie dodany nowy obiekt, który należy zatwierdzić przyciskiem Tak (Yes).

Po pomyślnej aktywacji rola będzie zainstalowana i uruchomiona.

22. Triki

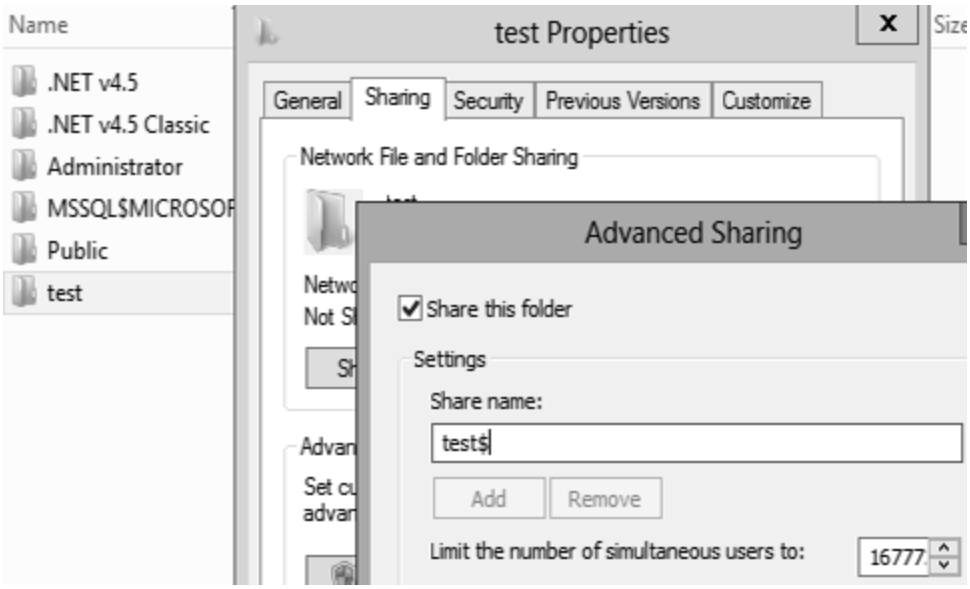
22.1. Wędrujący i wymuszony profil użytkownika

Należy stworzyć profil użytkownika, który nie będzie mógł samodzielnie edytować ustawień konta, a wprowadzone przez niego zmiany będą automatycznie kasowane. Na początku konieczne będzie stworzenia jakiegoś konta użytkownika, a następnie dostosowanie go do własnych

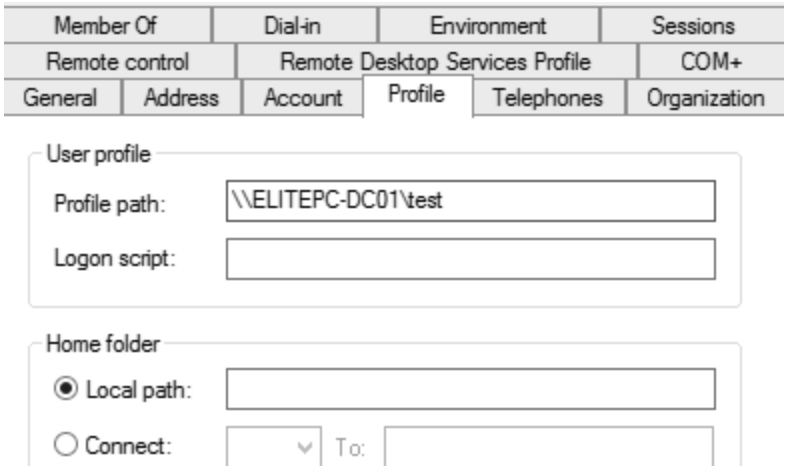
potrzeb. Kolejny krok to wylogowanie się z komputera i zalogowanie na nim jako administrator.

Dla przykładu, na samym początku można stworzyć nowy profil dla użytkownika „test”, a następnie zalogować się na nim po to, aby system utworzył jego domyślny profil. Można ten profil dostosować tak, aby spełniał odpowiednie oczekiwania (np. posiadał odpowiednie pliki czy skróty na pulpicie).

Później należy wylogować się z konta użytkownika „test” i zalogować jako administrator. Warto zauważyć, że na dysku lokalnym C, w folderze Users powstał nowy katalog o nazwie „test”. Powinien on zostać teraz udostępniony. Aby to uczynić, należy kliknąć w ten folder prawym klawiszem myszy i we właściwościach udostępnić go tak, aby tylko docelowa grupa użytkowników miała do niego dostęp. Warto też sprawić, aby folder był ukryty w otoczeniu sieciowym.

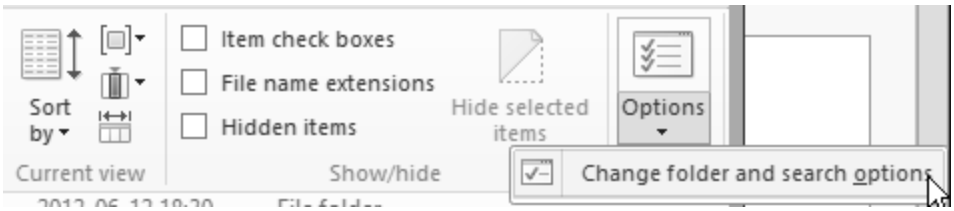


Potem należy otworzyć konsolę Użytkownicy i komputery usługi Active Directory (Active Directory Users and Computers). We właściwościach pożądanych użytkowników, w zakładce Profile podaje się ścieżkę dla profilu użytkownika (ścieżkę sieciową). Nie ma znaczenia, czy zostanie użyta adresacja IP, czy rekordy serwera DNS.



To jednak nie wszystko. Tak przygotowany profil użytkownicy będą mogli edytować i zapisywać w nim zmiany. Należy zmienić profil na tzw. Profil wymuszony (Mandatory). W tym celu w oknie zawierającym zawartość profilu użytkownika, w górnym menu należy kliknąć w guzik

Widok (View), następnie rozwinąć Opcje (Options) i wybrać Zmień opcje przeszukiwania folderów (Change folder and search options).

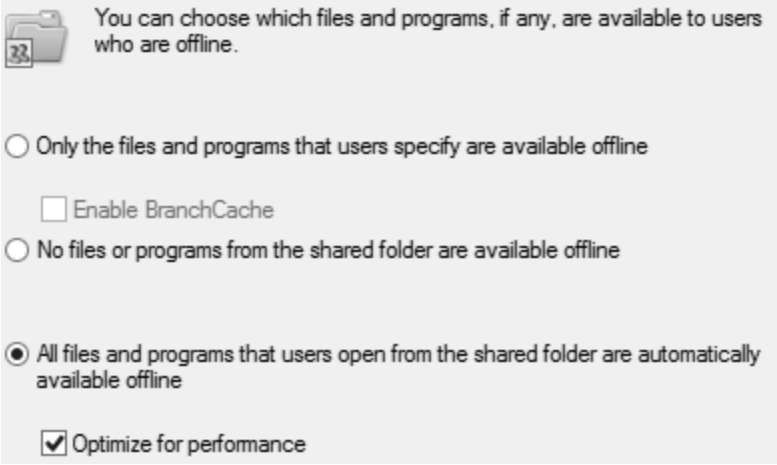


Teraz należy wejść w zakładkę Widok (View), gdzie należy wybrać Pokaż ukryte pliki i foldery (Show hidden files, folders and drives) i odznaczyć Ukryj rozszerzenie znanych typów plików (Hide extentions for known file types) oraz Ukryj chronione pliki systemowe (Hide protected operating system files).

W katalogu użytkownika pojawi się teraz więcej plików oraz ich rozszerzenia. Zmiana rozszerzenia pliku NTUSER.DAT na NTUSER.MAN spowoduje to, że żadne zmiany wprowadzone w profilu użytkownika, jak np. utworzenie nowego pliku na pulpicie czy zmiana tła pulpitu,

nie zostaną zachowane. Po wylogowaniu zmiany wprowadzone przez użytkownika zostaną utracone.

Obecna konfiguracja zakłada jednak to, że użytkownicy przy każdym logowaniu będą ściągali z serwera swoje dane. Jest to o tyle kłopotliwe, że może prowadzić do zbyt dużego obciążenia sieci. Wracając więc do właściwości udostępnionego folderu i uruchamiając jeszcze pliki trybu offline z optymalizacją dla wydajności, można osiągnąć to, że dane użytkowników będą ściągane nie zawsze, lecz np. wtedy, gdy użytkownik przesiądzie się na inny komputer. W przypadku zwykłych kont użytkownika również warto pomyśleć o takiej optymalizacji, jeżeli są one przechowywane w lokalizacji sieciowej.



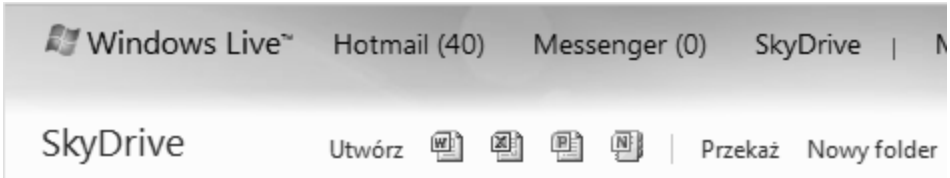
22.2. Dane w chmurze - mapowanie SkyDrive

Windows Live SkyDrive to wirtualny dysk autorstwa firmy Microsoft i jednocześnie część serwisu Windows Live. SkyDrive w darmowej wersji udostępnia 25 GB miejsca, ograniczeniem wysyłanych plików jest ich rozmiar nieprzekraczający 100 MB na plik (z racji nieustannie doskonalącej się oferty firmy Microsoft, liczby te mogą ulec zmianie). Te wartości jednak zmieniają się bardzo szybko.

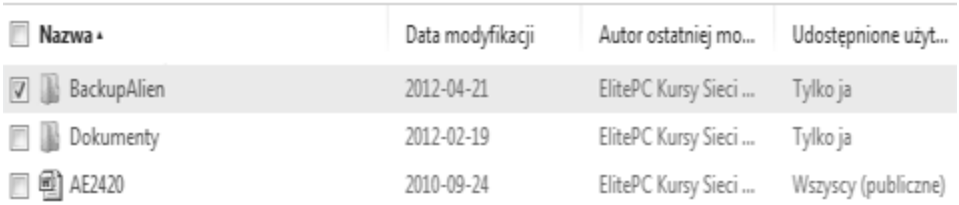
Teraz zostanie przedstawione, w jaki sposób podpiąć do swojego komputera lub serwera dysk SkyDrive, tak aby był widoczny w Moim komputerze, jak inne dyski. Dzięki temu będzie można zabezpieczyć w chmurze najważniejsze dane.

Analogiczne kroki można podjąć, posiadając wykupione płatne usługi w chmurze w firmie Microsoft. przykładzie przykładowa konfiguracja, dla ułatwienia, zostanie przedstawiona w przykładnie w systemie klienckim Windows 7. W innych systemach proces przebiega analogicznie.

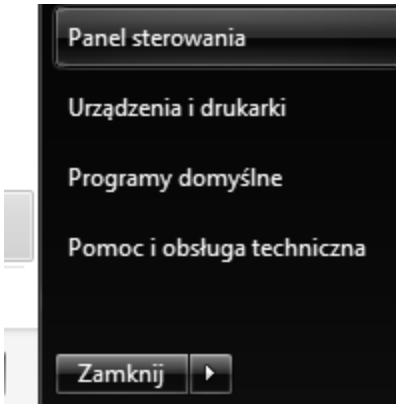
Pierwszym krokiem jest udanie się na stronę skydrive.live.com, gdzie należy albo się zalogować albo zarejestrować. Po zalogowaniu tworzy się folder bądź foldery.



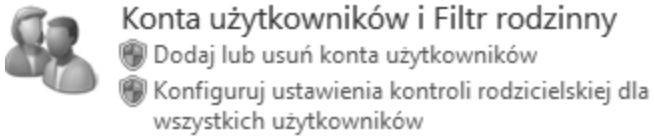
Warto zwrócić uwagę na to, by uprawnienia folderów były adekwatne do celu. Innymi słowy, jeżeli foldery nie mają być nikomu udostępniane, prawidłowym parametrem udostępniania powinno być „Tylko ja”.



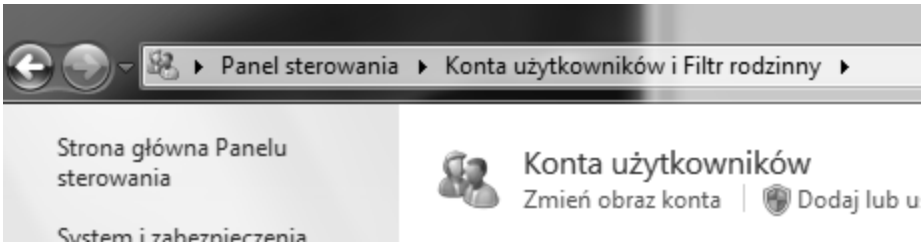
W Windows 7 należy wejść do Panelu sterowania.



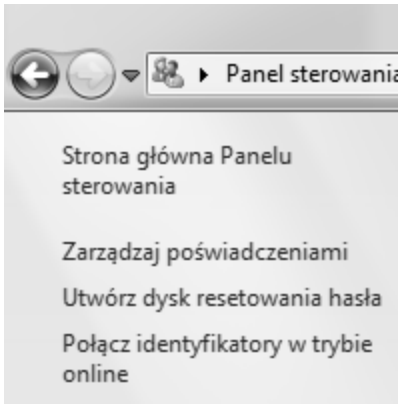
Następnie należy wybrać Konta użytkowników i Filtr rodzinny.



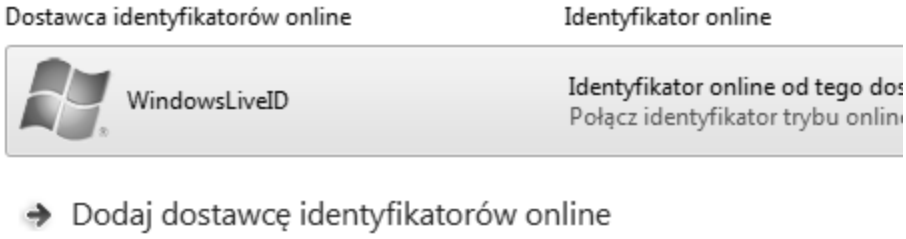
W dalszej kolejności konieczne jest wejście w Konta użytkowników.



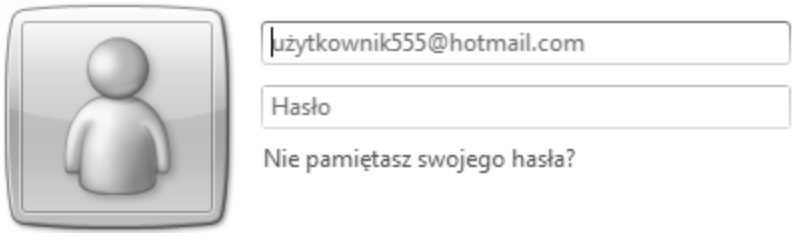
W końcu w menu, po lewej stronie okna należy kliknąć Połącz identyfikatory w trybie online.



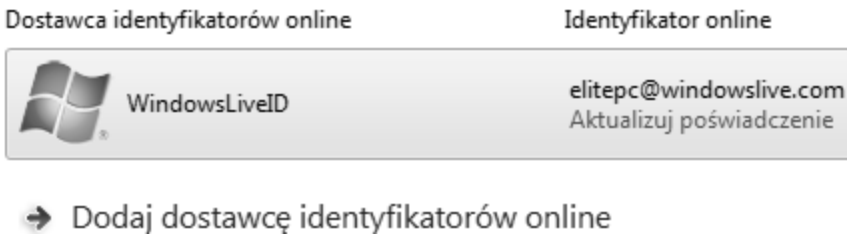
Na poziomie loga Windows Live ID konieczne jest kliknięcie w link Połącz identyfikator trybu online.



Jeżeli wgrane są dodatki Microsoft Live Essentials, pojawi się od razu ekran logowania do usługi Windows Live, w przeciwnym razie najpierw nastąpi przekierowanie do strony WWW, na której będzie możliwość pobrania niezbędnego pliku instalacyjnego.

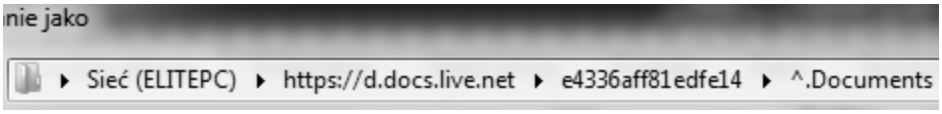


Po chwili oczekiwania pojawi się informacja o powiązaniu komputera z usługą Windows Live.

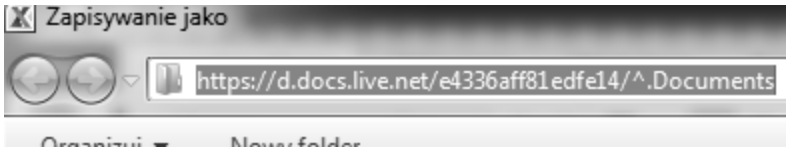


Teraz programy takie jak Microsoft Office uzyskały możliwość zapisu do dowolnego folderu na dysku SkyDrive. Aby taki folder zmapować, potrzebna będzie jego dokładna ścieżka sieciowa. W tym celu należy włączyć np. Excel, z menu Plik wybrać opcję Zapisz i Wyślij, a następnie w rozwiniętym menu Zapisz w sieci Web, aby po chwili z prawej strony pojawiły się foldery dostępne w usłudze SkyDrive. Konieczne jest wybranie folderu, który ma zostać zmapowany, i kliknięcie w Zapisz jako.

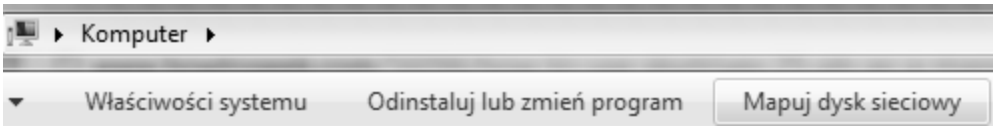
Po kliknięciu w górny pasek adresu pojawi się możliwość skopiowania adresu dysku.



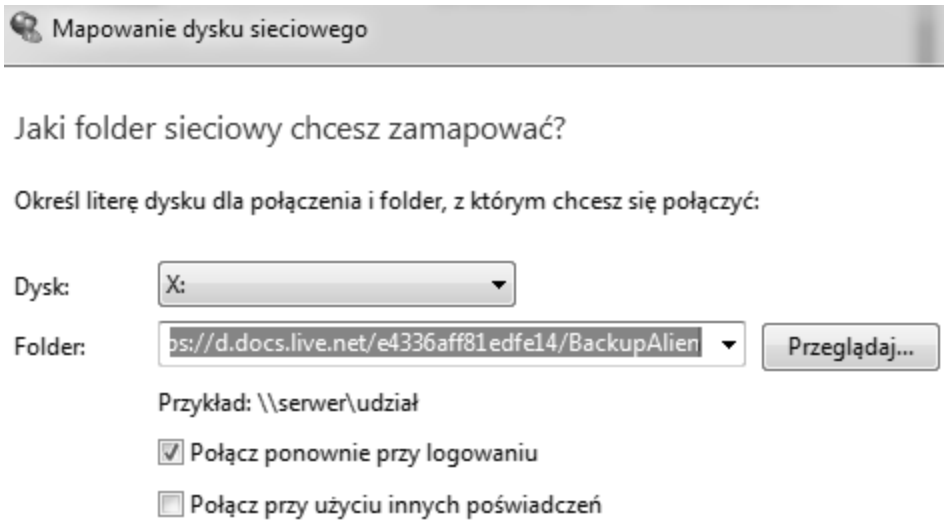
Po wyłuskaniu fizycznej ścieżki internetowej do dysku Skydrive, dysk ten można zamontować w tradycyjny sposób na dowolnym komputerze pod kontrolą Windows lub innego systemu operacyjnego.



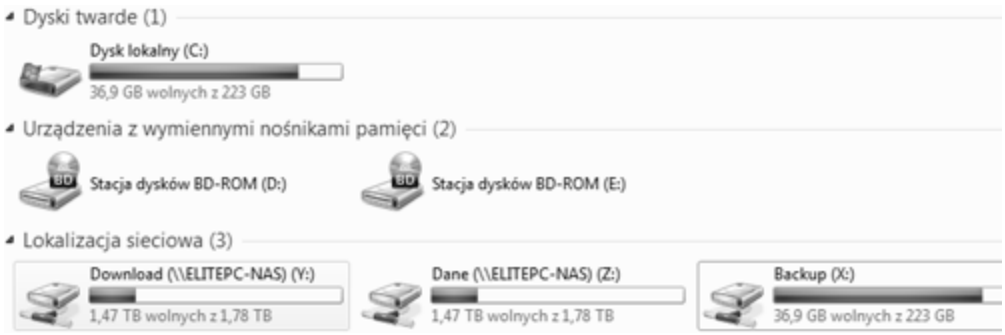
Należy wejść w Mój komputer i w górnym menu wybrać opcję Mapuj dysk sieciowy.



W oknie, które się pojawi, konieczne jest określenie litery dysku oraz wklejenie wcześniej skopiowanego linku. Całą akcję należy zatwierdzić, klikając Zakończ.



Jeżeli wszystko przebiegnie pomyślnie, dysk sieciowy pojawi się w Moim Komputerze i będzie automatycznie podłączany przy każdym uruchomianiu komputera. Teraz pozostaje tylko zabezpieczać swoje dane. Można to zrobić ręcznie bądź użyć np. darmowej aplikacji Comodo Backup.



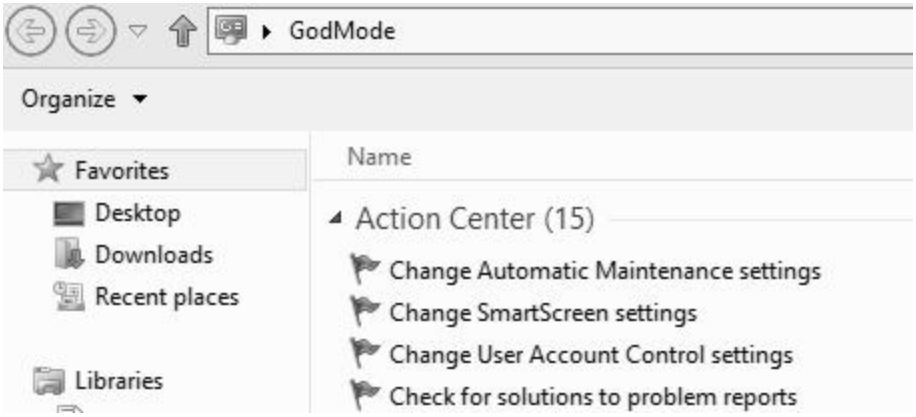
22.3. GodMode

W Windows Server 2016 można stworzyć specjalny folder, który pozwoli zebrać wszystkie narzędzia konfiguracyjne systemu w jednym miejscu. Aby utworzyć taki folder, należy postępować tak, jak w przypadku tworzenia zwykłego folderu, czyli kliknąć na pulpicie prawym klawiszem myszki i wybrać opcję Nowy > Folder, a następnie nadać nazwę folderowi, która musi być dokładnie taka jak poniżej:

GodMode.{ED7BA470-8E54-465E-825C-99712043E01C}

Folder został utworzony i zmieniła się jego ikona oraz nazwa, a mianowicie wygląda jak na ilustracji poniżej:

Jego zawartość jest imponująca i daje administratorowi duże możliwości wprowadzania przeróżnych konfiguracji dla systemu.



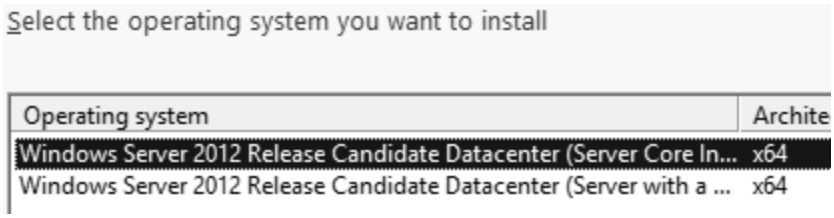
23. Windows 2016 bez GUI (wersja Core)

Windows Server 2016, podobnie jak jego poprzednik, może zostać zainstalowany w trybie Core. Tryb ten charakteryzuje się tym, że nie instaluje on graficznej powłoki systemu Windows. Nie są instalowane także programy korzystające z graficznego interfejsu użytkownika, za wyjątkiem kilku programów, jak na przykład notatnik. Systemem zainstalowanym w wersji Core można zarządzać za pomocą wiersza poleceń PowerShell’a lub zdalnie za pomocą Microsoft Management Console.

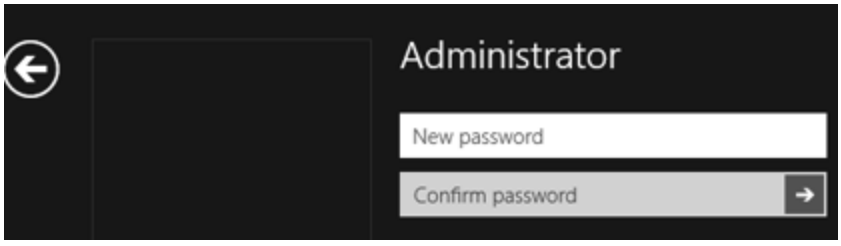
Z działu tego czytelnik dowie się, w jaki sposób zainstalować system w wersji Core oraz pozna podstawy zarządzania takim systemem na przykładzie kilku wybranych ról.

23.1. Instalacja wstępna konfiguracja

Proces instalacji systemu Windows Server 2016 w wersji Core praktycznie nie różni się od standardowej instalacji. Podczas wyboru systemu operacyjnego, który ma zostać zainstalowany, wystarczy wybrać ten, w którego nazwie w nawiasie występuje sformułowanie Server Core.



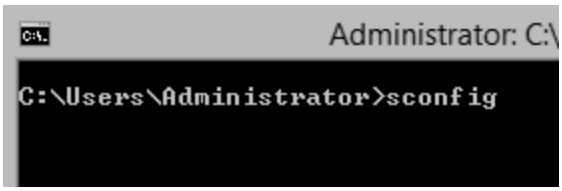
Pozostałe kroki instalatora są analogiczne do tych opisanych w rozdziale 1. Podobnie jak w tamtym rozdziale, instalator zakończy się prośbą o podanie nowego hasła dla administratora.



Podstawowym poleceniem, które będzie wykorzystywane, jest sconfig, które uruchamia Narzędzie konfiguracji serwera

(Server Configuration).

Podstawowym poleceniem, które będzie wykorzystywane jest sconfig, które uruchamia Narzędzie Konfiguracji Serwera (Server Configuration).

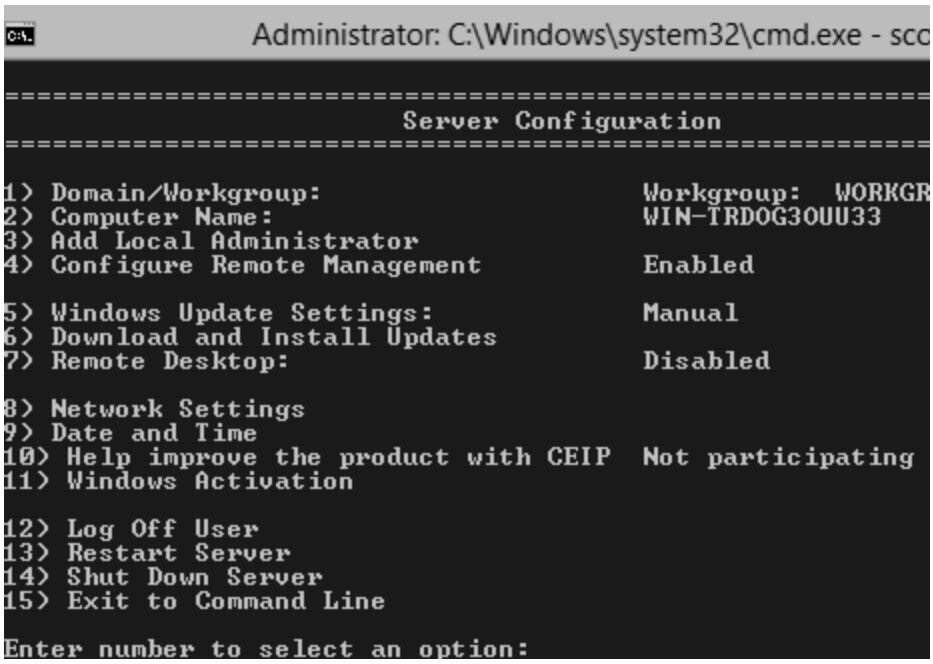


Narzędzie to pozwala na konfigurację podstawowych ustawień komputera takich jak:

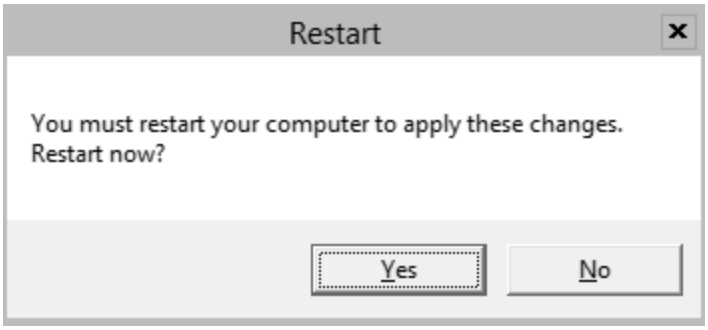
- Domena/grupa robocza,
- Nazwa komputera,
- Dodawanie administratorów,
- Konfigurowanie zdalnego zarządzanie,
- Konfigurowanie aktualizacji,
- Ściągnięcie i instalacja aktualizacji,
- Zdalny pulpit,
- Ustawienia sieci,
- Ustawienia daty i czasu,
- Konfiguracja ustawień związanych z programem raportowania błędów w firmie Microsoft,
- Aktywacja systemu,
- Wylogowanie użytkownika,

- Ponowne uruchomienie serwera,
- Wyłączenie serwera,
- Wyjście do wiersza poleceń.

Aby dostać się do jakichś ustawień, wystarczy podać numer wybranej opcji, a wybór zatwierdzić klawiszem Enter.

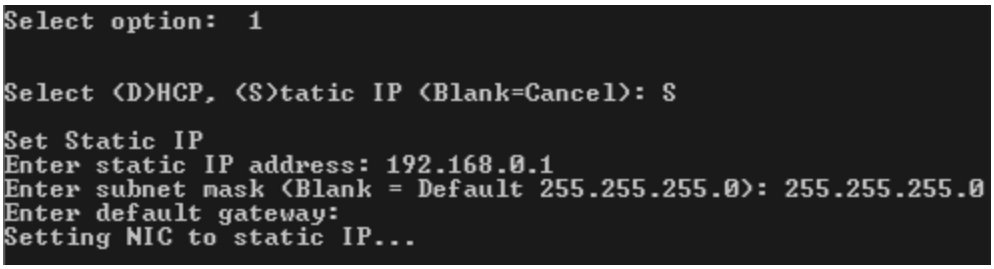


Pierwszym krokiem będzie nadanie komputerowi odpowiedniej nazwy. Dokonuje się tego poprzez wybranie opcji numer 2 i wprowadzenie pożądanej nazwy komputera. Po zatwierdzeniu jej klawiszem Enter pojawi się okienko informujące o tym, że wymagany jest ponowny rozruch komputera.

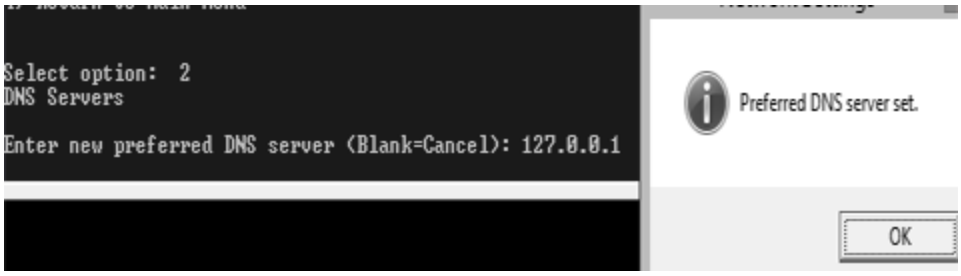


Gdy komputer ponownie się uruchomi, należy włączyć narzędzie konfiguracji serwera, aby tym razem skonfigurować sieć za pomocą opcji numer 8. Po jej wybraniu wyświetlona w formie listy zostanie tablica dostępnych interfejsów sieciowych. Aby dostać się do konfiguracji któregoś z nich, należy podać jego indeks, a wybór potwierdzić przyciskiem Enter. Do wyboru pojawią się cztery opcje. Są nimi: konfiguracja adresów sieciowych, konfiguracja serwerów DNS, oczyszczenie ustawień serwerów DNS oraz powrót do poprzedniego menu.

Za pomocą opcji pierwszej należy przypisać serwerowi statyczny adres IP. Komputer najpierw zapyta, czy adres IP ma być przypisywany z serwera DHCP (opcja D), czy adres będzie statycznych (opcja S). Następnie poprosi o wprowadzenie kolejnych adresów IP. Jeżeli jakieś mają nie zostać podane, zostawia się pole puste.



Należy także skonfigurować serwery DNS, jeżeli będą takowe wymagane. W przykładowym laboratoryjnym przypadku Windows Server sam w sobie będzie serwerem DNS, więc należy wprowadzić adres IP localhosta, czyli 127.0.0.1.



Oprócz korzystania z poleceń PowerShell'a oraz przygotowanych programów, można korzystać także z wiersza poleceń. Za pomocą polecenia md Share należy stworzyć na dysku C komputera folder o nazwie Share. Poleceniem dir należy wyświetlić w formie listy zawartość dysku C w celu weryfikacji, czy folder został utworzony.

Aby folder udostępnić, należy wydać polecenie NET SHARE z odpowiednim parametrem.

Naturalnie, poznanie wszystkich poleceń oraz wszystkich możliwych parametrów jest tematem na kilka oddzielnych publikacji. Tym, o czym będzie teraz wspomniane, jest możliwość skorzystania z podpowiedzi dla każdej z komend, które można wyświetlić za pomocą sformułowania nazwa_polecenia /?

23.2. Zarządzanie systemem w wersji Core

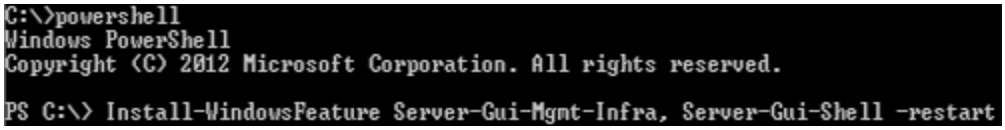
W tym podrozdziale największa waga zostanie przywiązana do nauki podstaw zarządzania systemem Windows Server 2016 w wersji Core. Przede wszystkim zostaną przedstawione różne interfejsy użytkowników oraz możliwości przełączania się między nimi, a także różnice między poszczególnymi interfejsami. Następnie zostanie zainstalowanych kilka podstawowych ról serwera za pomocą wiersza poleceń zamiast trybu graficznego.

.

23.2.1. Interfejsy użytkownika

Jedną z nowości w Windows Server 2016 jest możliwość swobodnego przełączania się pomiędzy graficznym a tekstowym interfejsem użytkownika. Aby tego dokonać,

wymagany będzie jedynie restart komputera. Wcześniej taka zmiana wymagała reinstalowania całego systemu operacyjnego. Jest to ukłon w stronę administratorów, którzy są początkujący w PowerShell i pragną dokonać konfiguracji w trybie graficznym, a następnie przełączyć się do trybu tekstowego, dzięki czemu serwer nie straci na prostocie konfiguracji, a jednocześnie będzie lepiej zabezpieczony. Żeby przełączyć się z trybu tekstowego na graficzny, należy wydać polecenie: Install-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell –Restart. Przed jego wpisaniem należy uruchomić PowerShell komendą powershell.

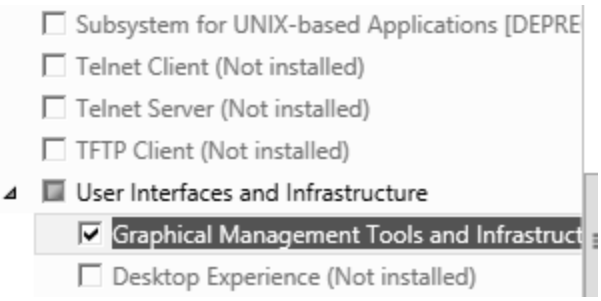


Rozpocznie się proces instalacji i pojawi się pasek postępu. Instalacja może trwać od kilku do kilkunastu minut w zależności od wydajności komputera.

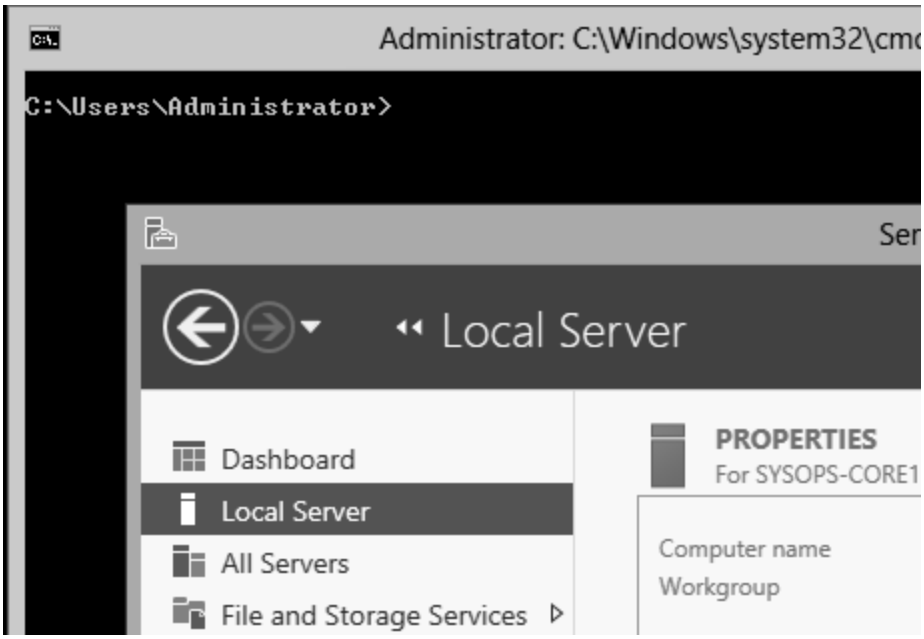
Aby z trybu graficznego powrócić do trybu tekstowego, należy wpisać polecenie Uninstall-WindowsFeature Server-Gui-Mgmt-Infra –Restart.

W Windows Server 2016 została jeszcze wprowadzona opcja pośrednia, tzw. Minimalny interfejs serwera (Minimal Server Interface), zwany również MinShell. Stanowi on coś pośredniego pomiędzy trybem w pełni graficznym a w pełni tekstowym. Administrator w tym trybie ma dostęp do

graficznej konsoli Menadżera serwera. W części panelu sterowania konsoli MMC oraz wiersza poleceń PowerShell administrator nie ma dostępu do Explorera Windows, Internet Explorera oraz interfejsu startowego metra. Poza zwiększeniem wygody, MinShell zwiększa także bezpieczeństwo systemu Windows Server, zmniejszając obszary potencjalnych ataków. Aby uruchomić system operacyjny w tym trybie, należy odinstalować wszystkie role i funkcje z wyjątkiem Graphical Management Tools and Infrastructure. Kolejnym krokiem będzie ponowne uruchomienie komputera.



Po ponownym uruchomieniu komputera interfejs, który się wczyta, będzie hybrydowy. Pojawią się zarówno elementy z trybu graficznego, jak i tekstowego.



23.2.2. Podstawowe role serwera

Windows Server 2016 daje możliwość instalacji większej ilości ról niż w przypadku swoich poprzedników. Oprócz tego wprowadza większą liczbę poleceń PowerShell. Nowością jest także możliwość instalacji Microsoft SQL Server 2016 w serwerze w wersji Core, co znaczy, że serwer IIS ma możliwość hostowania aplikacji ASP.NET. Możliwe do zainstalowania role to:

- Active Directory Certificate Services (AD CS),
- Active Directory Domain Services (AD DS),
- Active Directory Lightweight Directory Services (AD LDS),

- Active Directory Rights Management Server (AD RMS),
- DHCP Server,
- DNS Server,
- File and Storage Services,
- Hyper-V,
- Print and Document Services,
- Remote Desktop Services (RDS):
    - Remote Desktop Connection Broker,
    - Remote Desktop Licensing,
    - Remote Desktop Virtualization Host,
- Routing and Remote Access Server (RRAS),
- Web Server,
- Windows Server Update Server (WSUS).

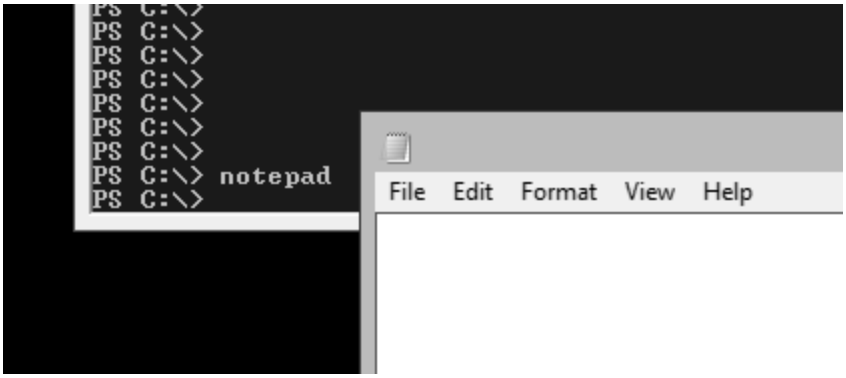
Windows Server 2008 dawał możliwość instalacji następujących ról:

- Active Directory Domain Services (AD DS),
- Active Directory Certificate Services (AD CS),
- Active Directory Lightweight Directory Services (AD LDS),
- DHCP Server,
- DNS Server,
- File Services,
- Print Services,
- Streaming Media Services,
- Internet Information Services (IIS),

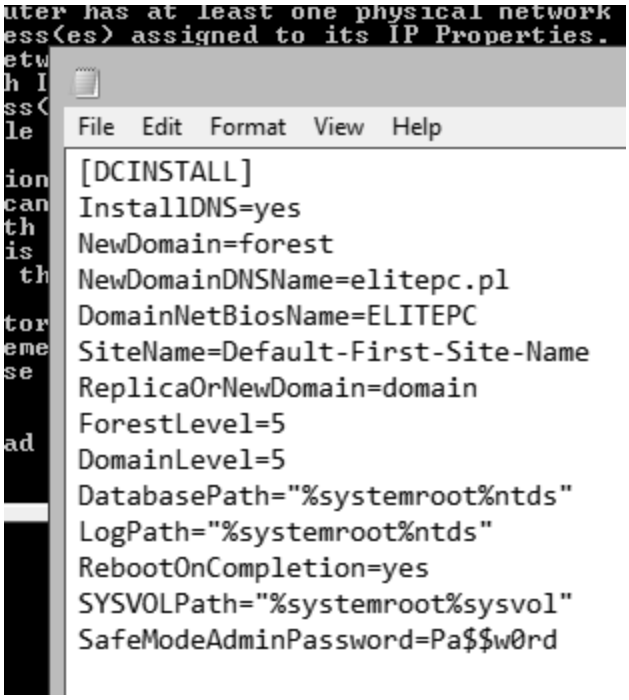
- Hyper-V.

24. Nienadzorowana instalacja Active Directory

Podobnie jak w przypadku trybu graficznego, należy wcześniej skonfigurować odpowiednią nazwę komputera oraz adresację IP. Aby instalacja przebiegła pomyślnie, niezbędny będzie serwer DNS. Wprawdzie Windows Server 2016 wprowadza nowe narzędzie konfiguracji domeny, jednak podejście znane ze starszych wersji Windows Server również się sprawdzi.



Pierwszym krokiem będzie uruchomienie notatnika poleceniem notepad w celu przygotowania pliku konfiguracyjnego dla nienadzorowanej instalacji. To z niego instalator pobierze informacje i w sposób automatyczny przeprowadzi awans serwera do pierwszego kontrolera domeny w nowym lesie.

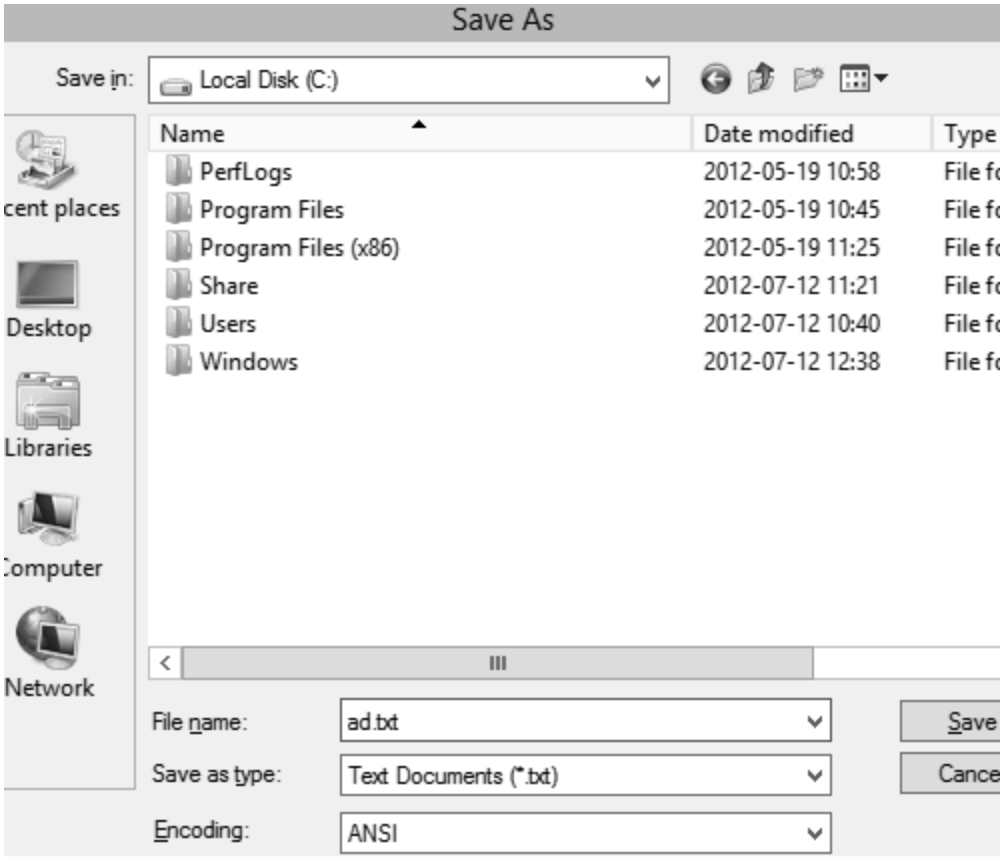


Plik tekstowy powinien zaczynać się poleceniem DCINSTALL, które mówi o tym, jakiego typu dane się tutaj znajdują. Kolejne wiersze tego pliku to polecenia odpowiadające kolejno za:

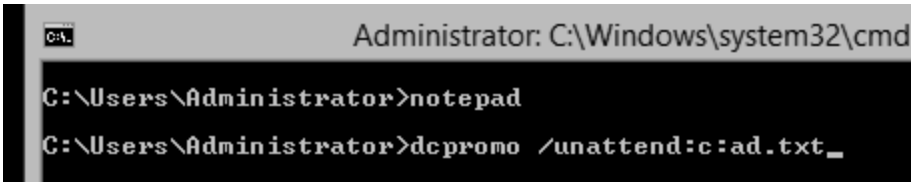
- Określenie czy ma być zainstalowany serwer DNS,
- Określenie czy tworzony jest nowy las czy nowa domena,
- Określenie DNSowej nazwy domeny,
- Określenie netbiosowej nazwy domeny,
- Nazwa lokalizacji,
- Określenie czy tworzona jest nowa domena czy replika,
- Określenie poziomu funkcjonalności lasu (1 – Windows 2000, 2 – Windows 2003, 3 – Windows 2008, 4 – Windows 2008 R2, 5 – Windows 2016),
- Określenie poziomu funkcjonalności domeny,
- Lokalizacja bazy danych,

- Lokalizacja logów,
- Zgoda na zresetowanie komputera po zakończeniu,
- Lokalizacja folderu Sysvol,
- Hasło administratora trybu przywracania.

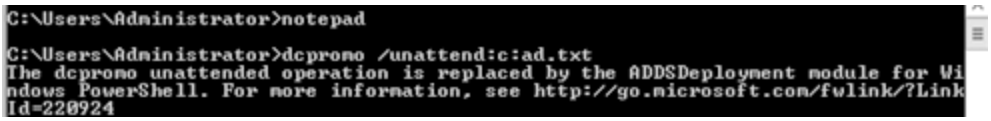
Tak przygotowany plik należy zachować na dysku C, np. AD.txt.



Kolejnym krokiem jest podanie polecenia dcpromo /unattend:c:unattend.txt.



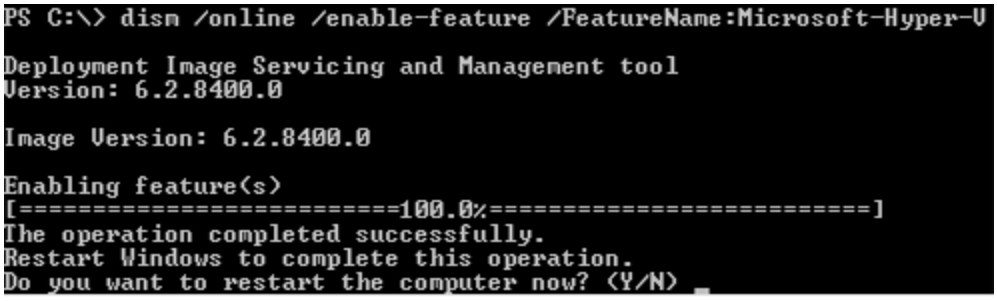
Pojawi się informacja o tym, że dcpromo zostało zastąpione przez ADDSDeployment, a instalacja będzie kontynuowana. Niezbędny stanie się ponowny rozruch komputera. Gdy to nastąpi, Windows Server będzie miał zainstalowaną rolę DNS oraz Active Directory Domain Services.



Następnym krokiem będzie instalacja serwera DHCP przy użyciu PowerShell. Po uruchomieniu konsoli PowerShell należy wydać polecenie Add-WindowsFeature DHCP.

Rola serwera DHCP została zainstalowana. Należy jedynie ją skonfigurować.

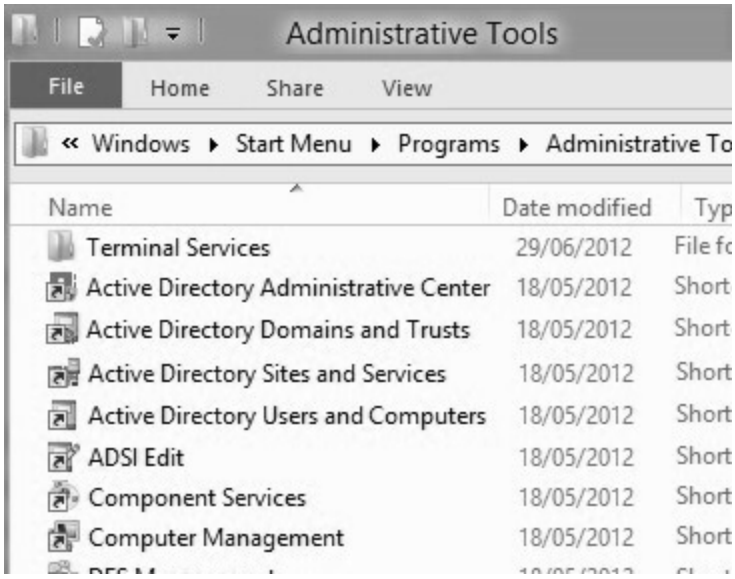
Inną rolą, którą warto zainstalować na serwerze w wersji Core, jest Hyper-V. Służy temu polecenie dism /online /enable-feature /FeatureName:Microsoft-Hyper-V.



W analogiczny sposób można zainstalować pozostałe role serwera. Każdą z tych ról można zarządzać na kilka sposobów, ponieważ każda rola posiada szereg poleceń PowerShell służących do zarządzania nimi. Po więcej

informacji w tej materii warto zajrzeć na stronę Microsoft Technet. Innym sposobem zarządzania jest zarządzanie z poziomu Menadżera Serwera na innej maszynie z systemem Windows Server bądź za pomocą dodatku na stacje robocze zwanego Narzędziami Administracyjnymi Serwera (Remote Server Administration Tools).

Pakiet Administration Tools można znaleźć za darmo w Internecie bądź na płycie instalacyjnej Windows Server.



Zawiera on przygotowane konsole, po włączeniu których, za pomocą adresu IP, nastąpi połączenie się z serwerem. Jest to sposób wygodny i bezpieczny, pozwalający także na zdalne zarządzanie nawet spoza przedsiębiorstwa przy użyciu połączenia VPN.

25. Migracja z Windows Server 2003

Wymagania wstępne:

1. Należy się upewnić, że oba serwery są zaktualizowane do najnowszej wersji Service Pack.

2. Należy się upewnić, że serwer Windows 2003 jest na poprawnym poziomie funkcjonalnym.

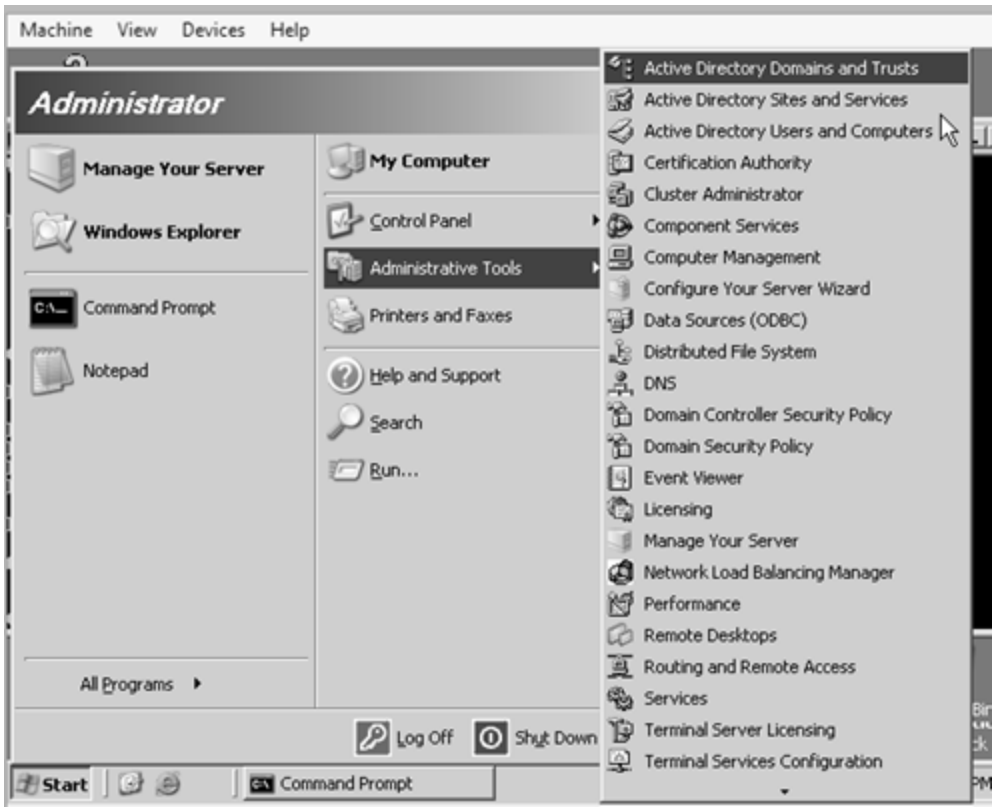
3. Jeżeli nie jest, trzeba podnieś poziom domeny do Windows Server 2003.

4. Poziom domeny nie musi być podniesiony w przypadku, gdy jest prawidłowy.

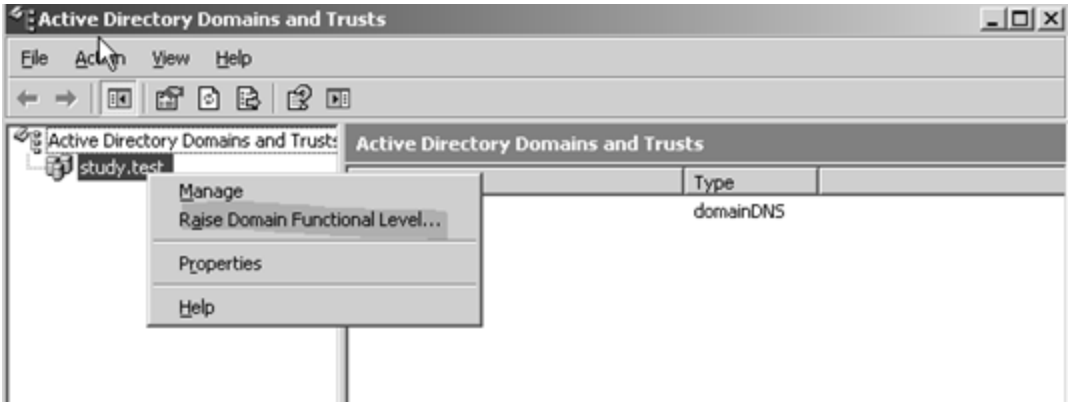
5. Na końcu należy się upewnić, że jesteśmy członkiem Enterprise Admins Group w AD.

25.1. Podnoszenie Domain Functional Level

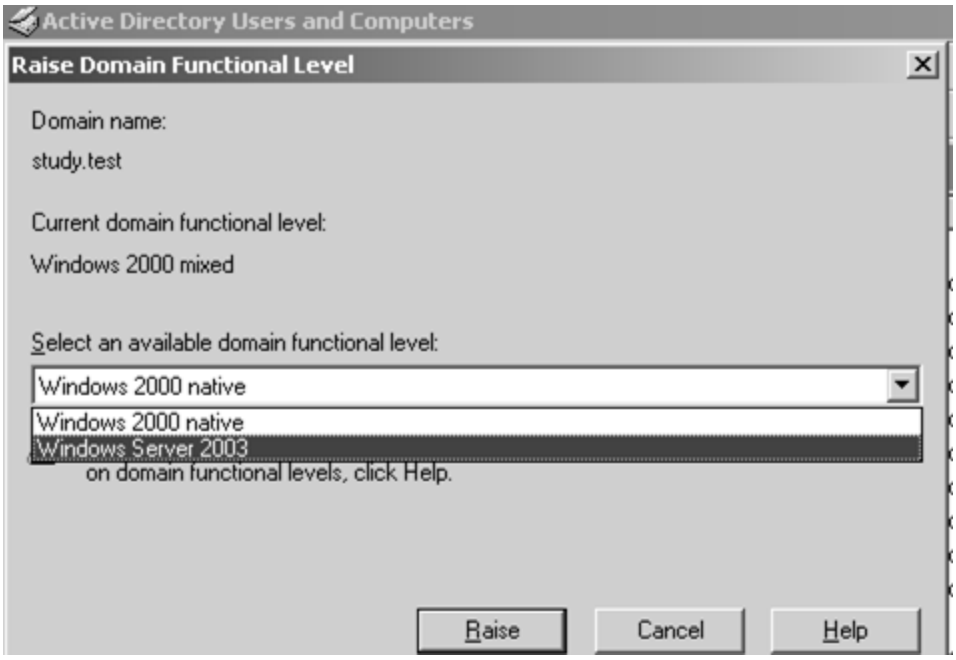
Należy przejść do Active Directory Domains and Trusts.



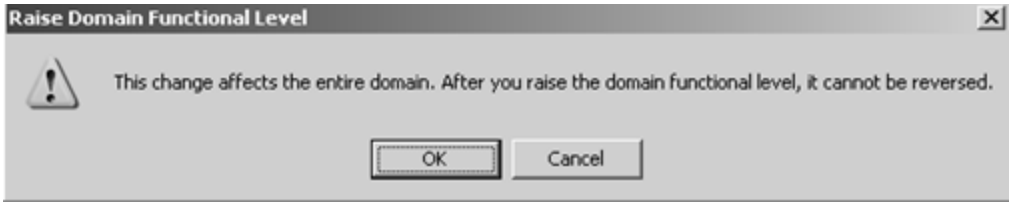
Następnie nacisnąć prawym przyciskiem myszy na kontrolerze domeny i kliknąć Raise Domain Functional Level.



Kolejnym krokiem jest wybór Domain Functional Level, jako Windows Server 2003.



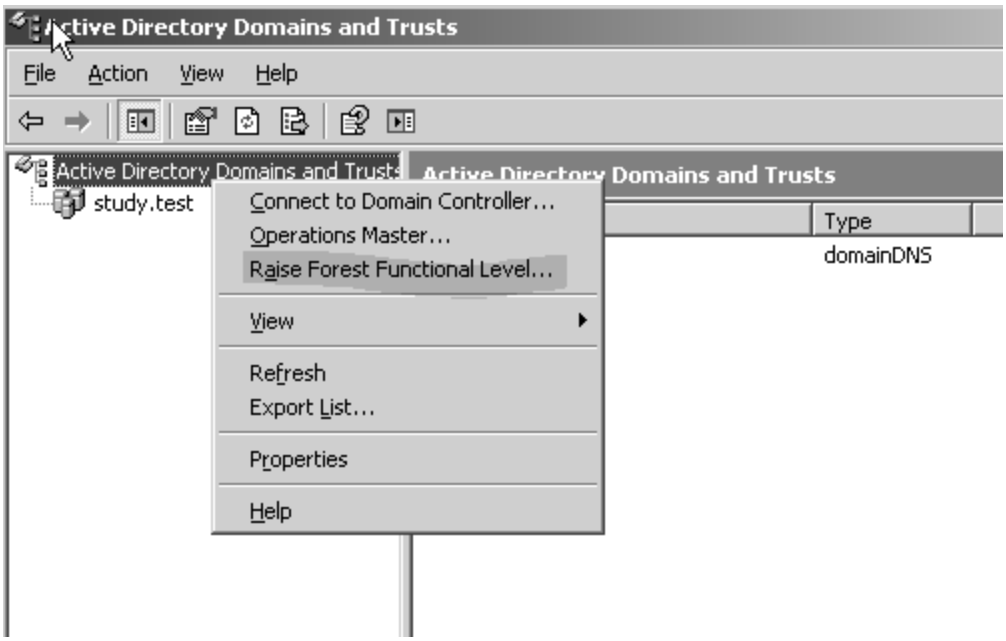
Należy kliknąć Raise i OK.



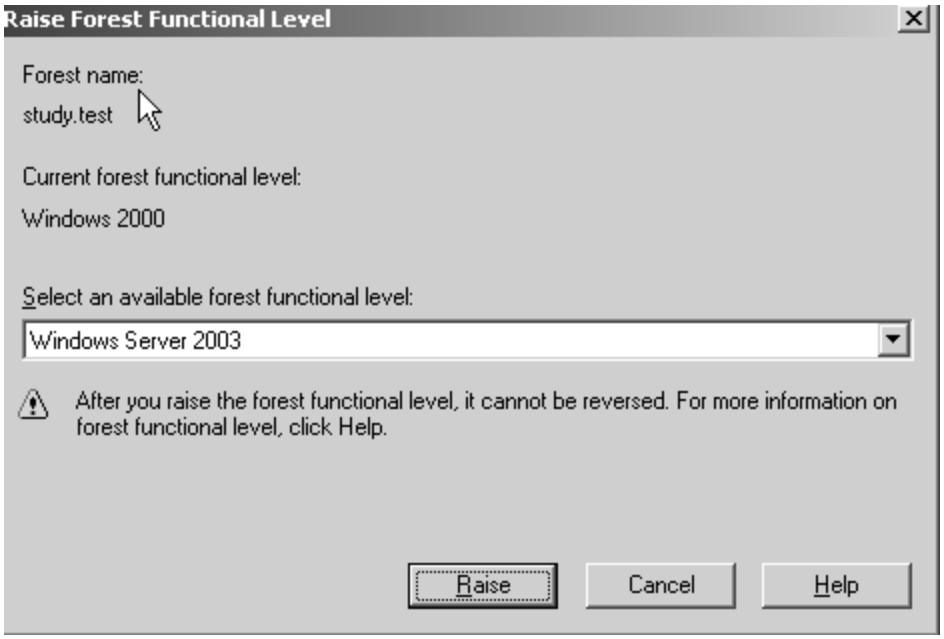
I ponownie kliknąć OK.

Można kliknąć prawym przyciskiem myszy na kontrolerze domeny, po czym kliknąć na Raise Domain Controller, aby potwierdzić poziom domeny. Teraz jest on na Windows Server 2003.

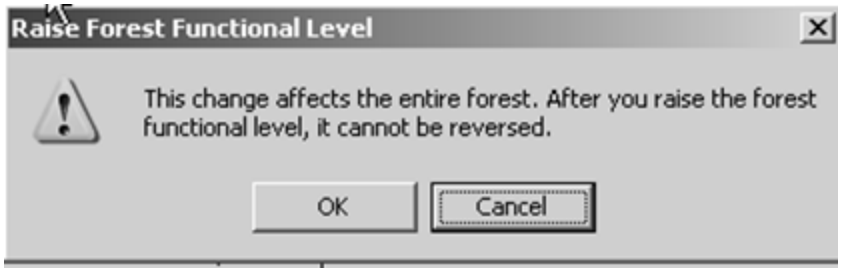
Następnie należy nacisnąć prawym przyciskiem myszy na Active Directory Domains and Trusts, po czym kliknąć Raise Forest functional Level.



Następnie trzeba wybrać Windows 2003 i kliknąć Raise.



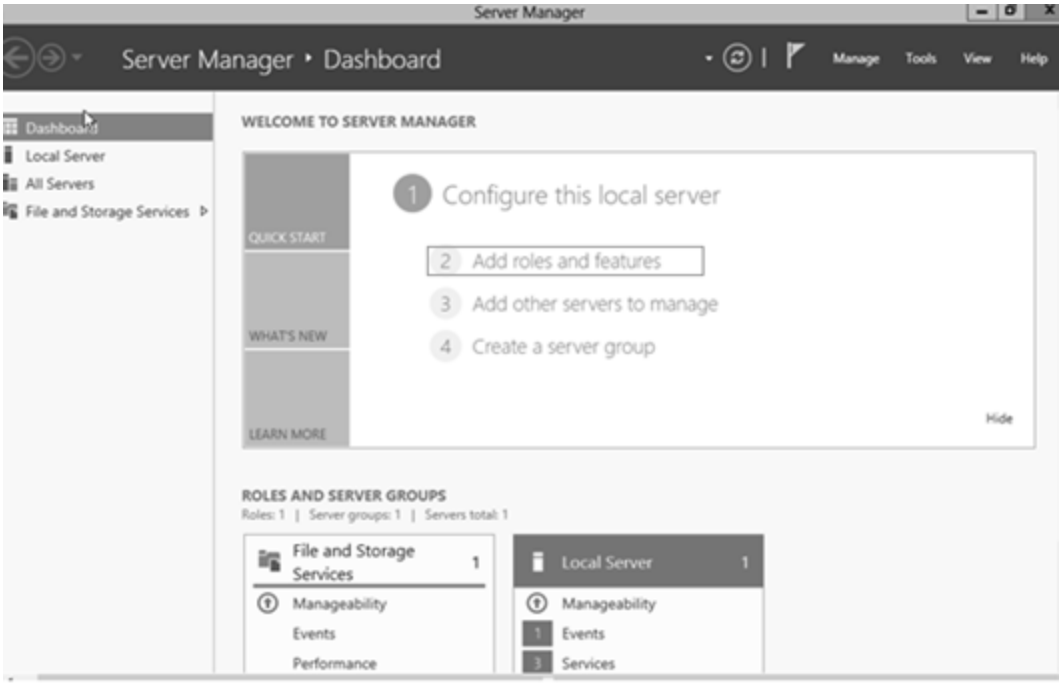
Następnie należy kliknąć OK.



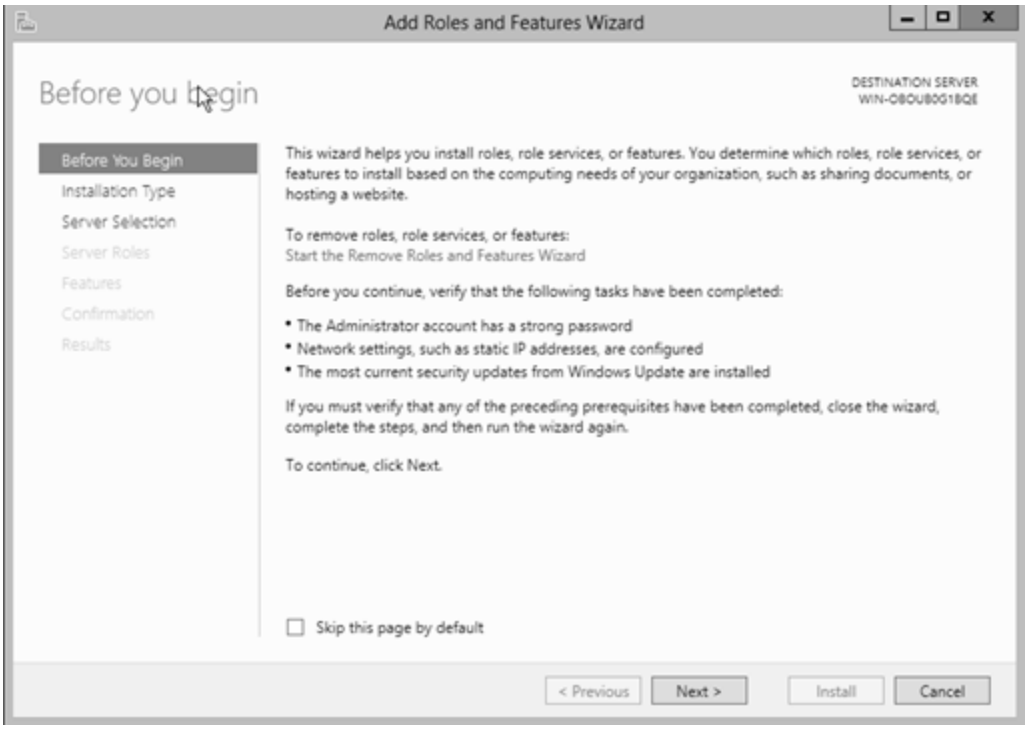
Ponownie należy kliknąć OK.

26. Instalowanie Active Directory Role na Windows Server 2012

Na początku należy zalogować się do windows Server 2012 i przejść do Server Manager, a następnie kliknać Add Roles and features.

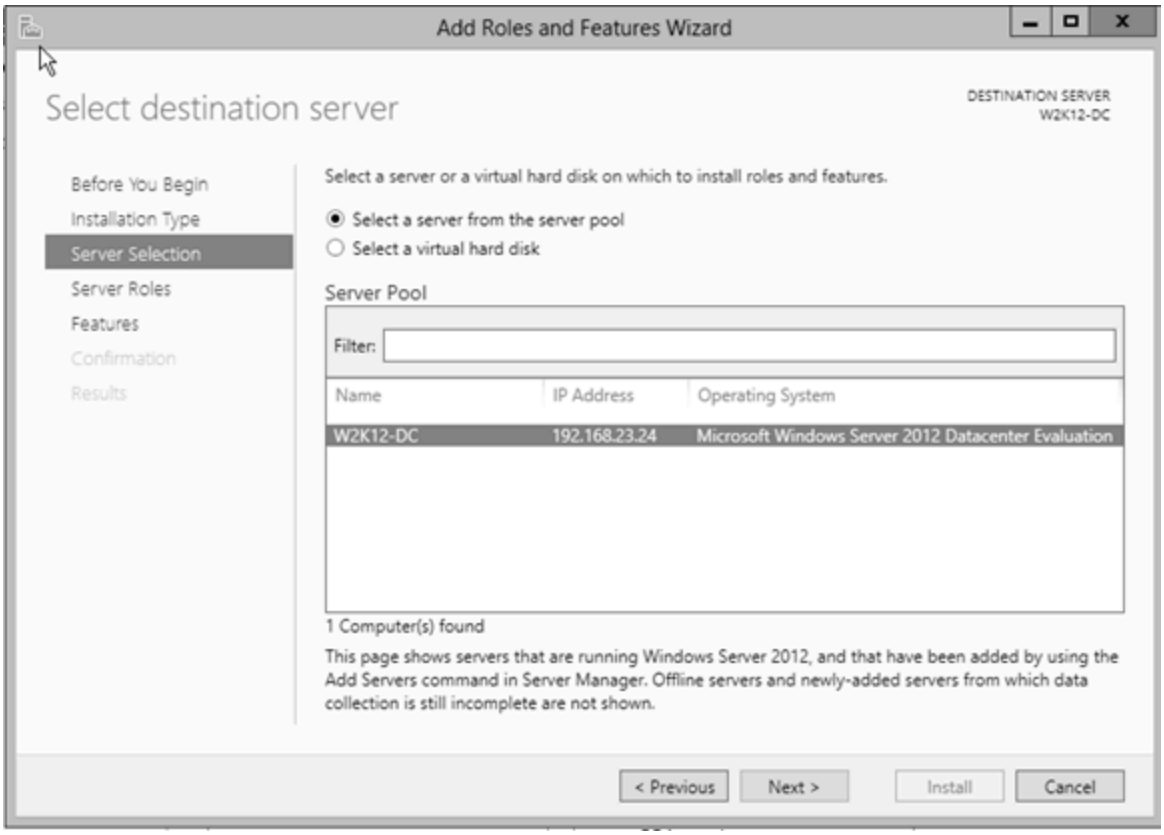


Należy kliknąć Next.

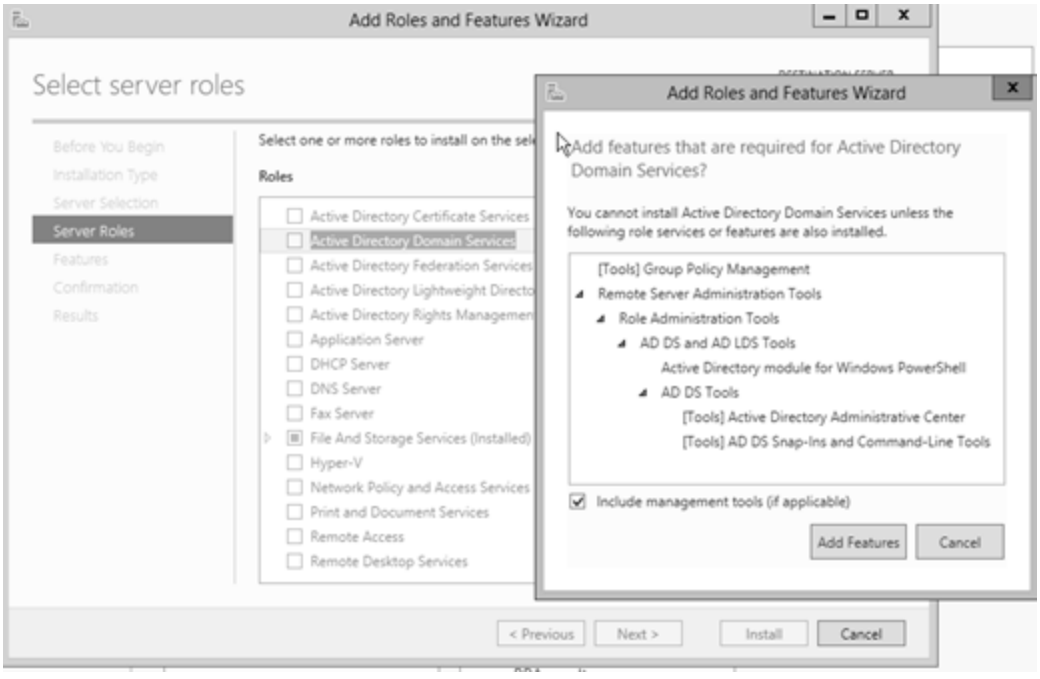


W kolejnym oknie trzeba zaznaczyć Role based on feature-based installation.

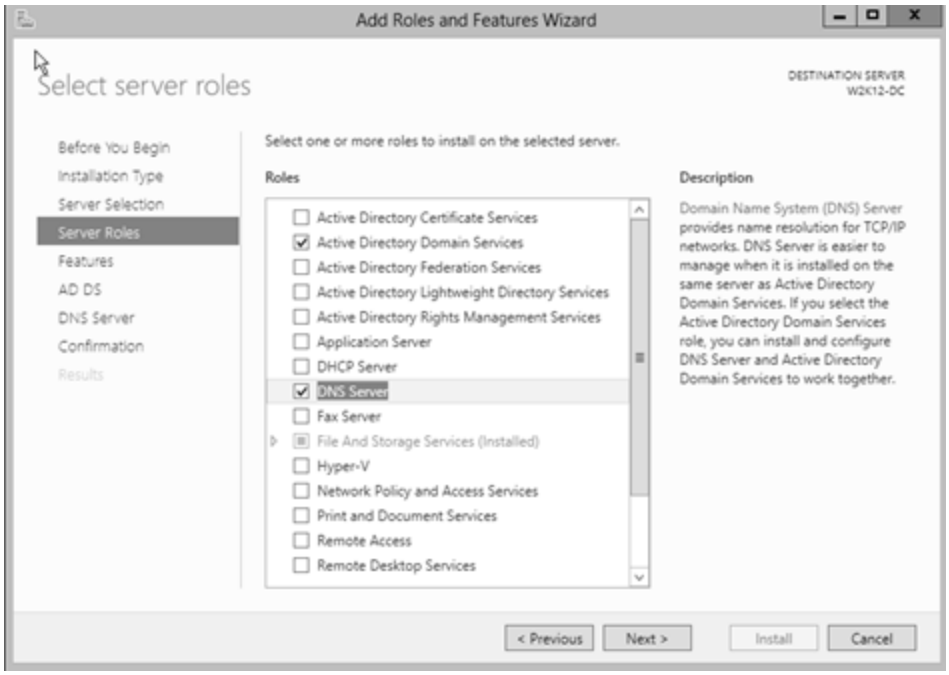
Aby przejść dalej, trzeba zaznaczyć Windows Server 2012 i kliknąć Next.



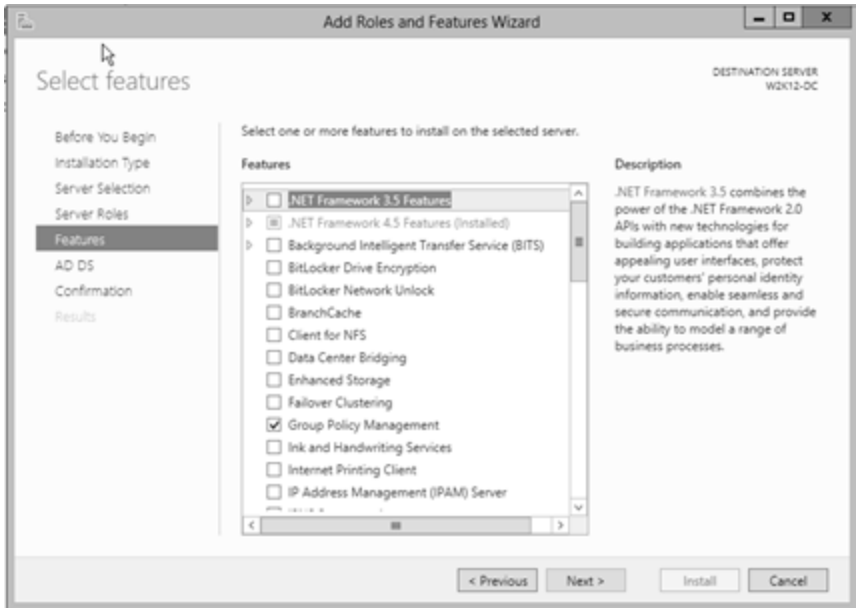
Następnie trzeba zaznaczyć Active Directory Domain Services i kliknąć Add Features.



Należy kliknąć Next i wybrać DNS server.



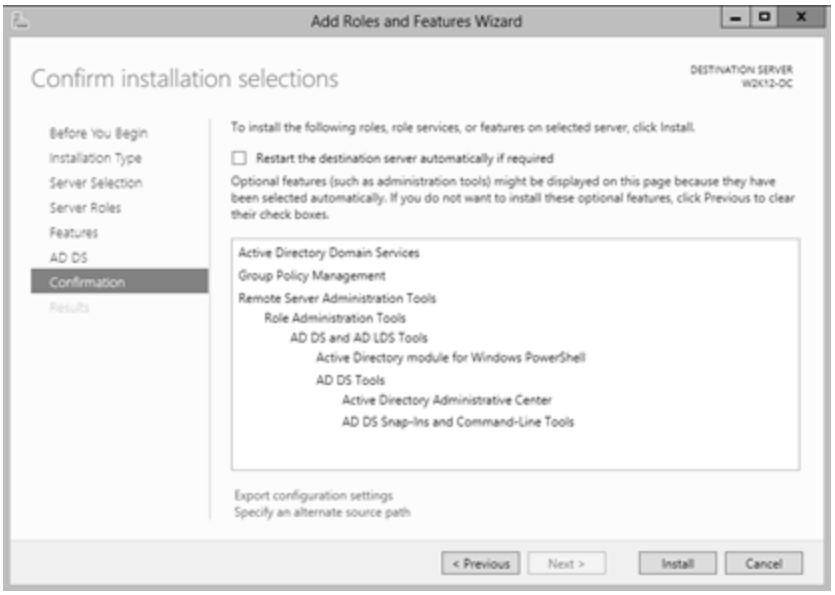
Znów należy Next.



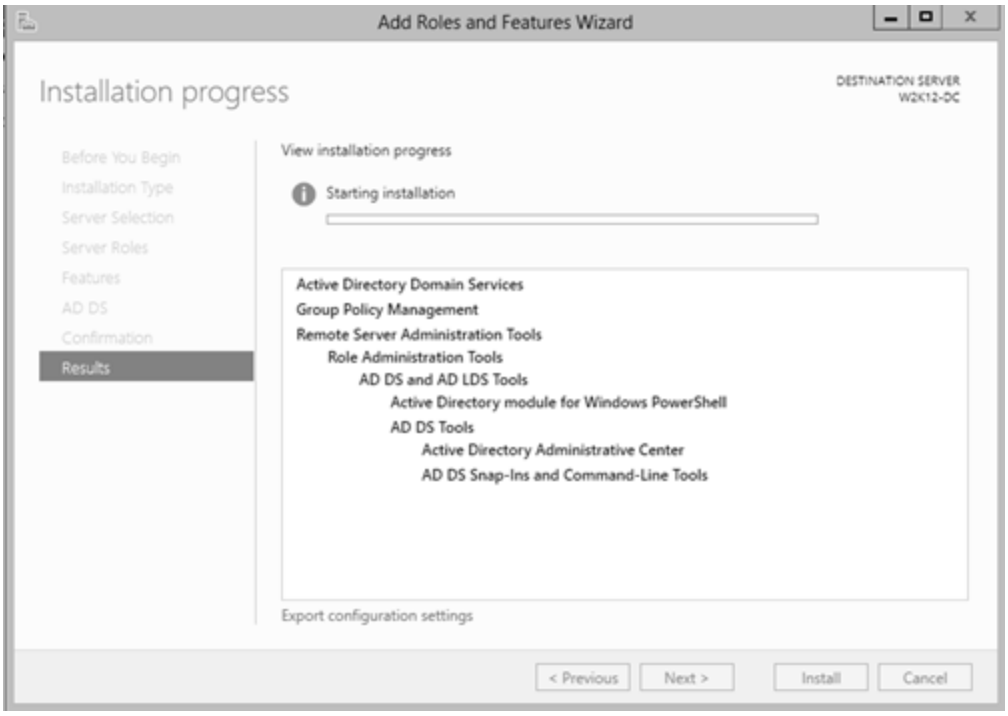
I ponownie trzeba kliknąć Next.

W kolejnym oknie znów należy klinąć Next.

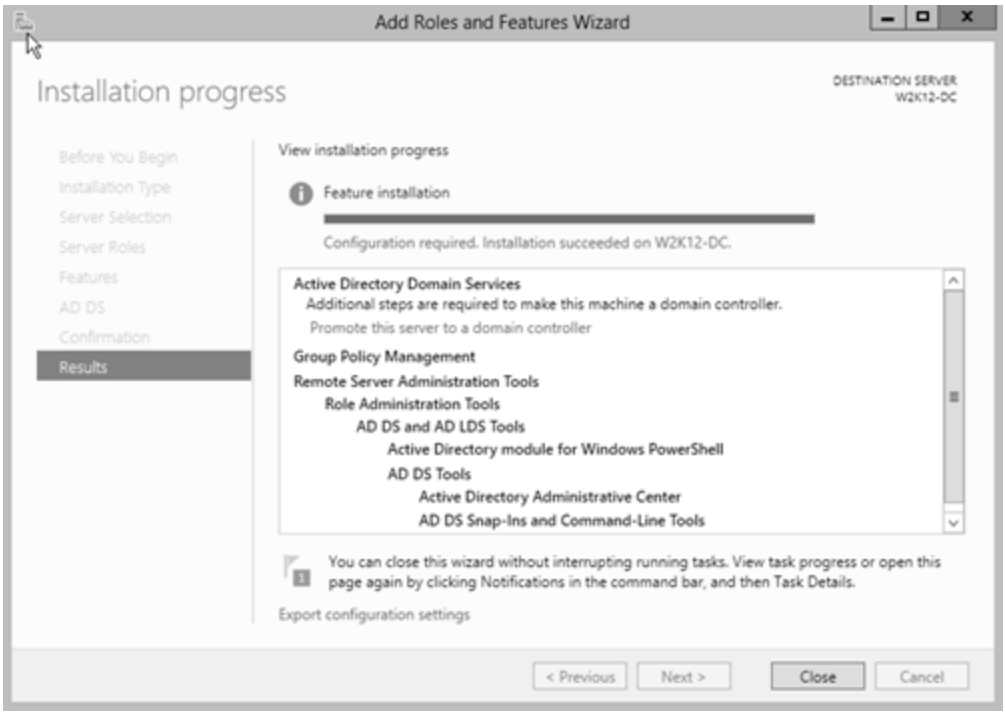
Kolejnym krokiem jest kliknięcie przycisku Install.



Należy poczekać, aż proces instalacji zostanie zakończony. Można zamknąć to okno i obserwować postęp na pasku powiadomień.

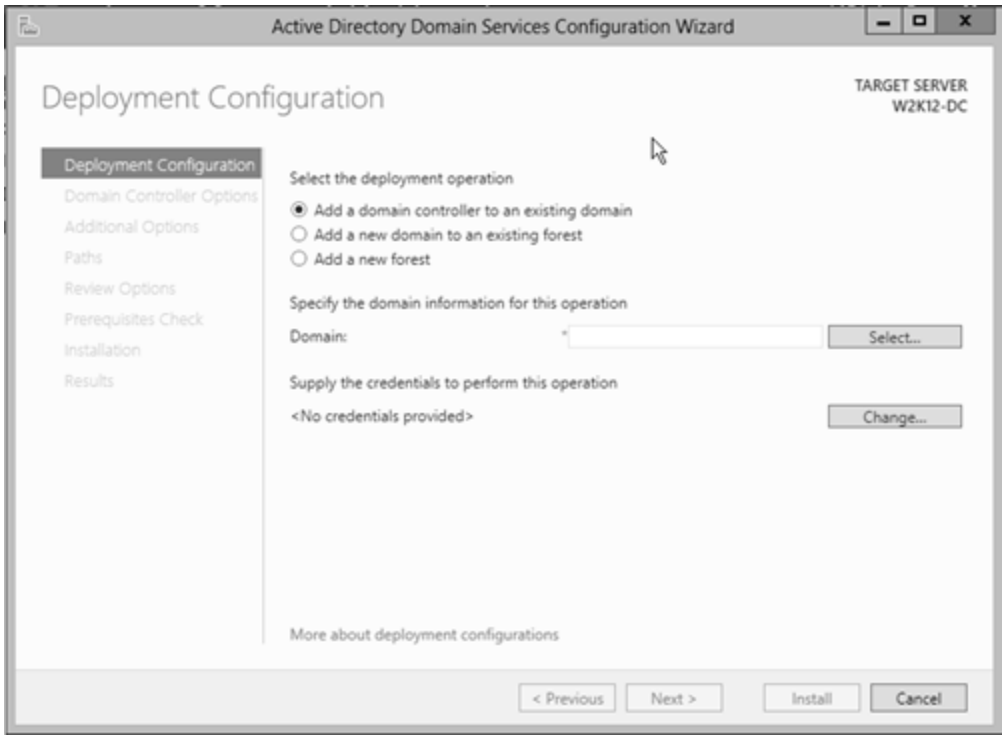


Gdy instalacja się zakończy, należy kliknąć Close.

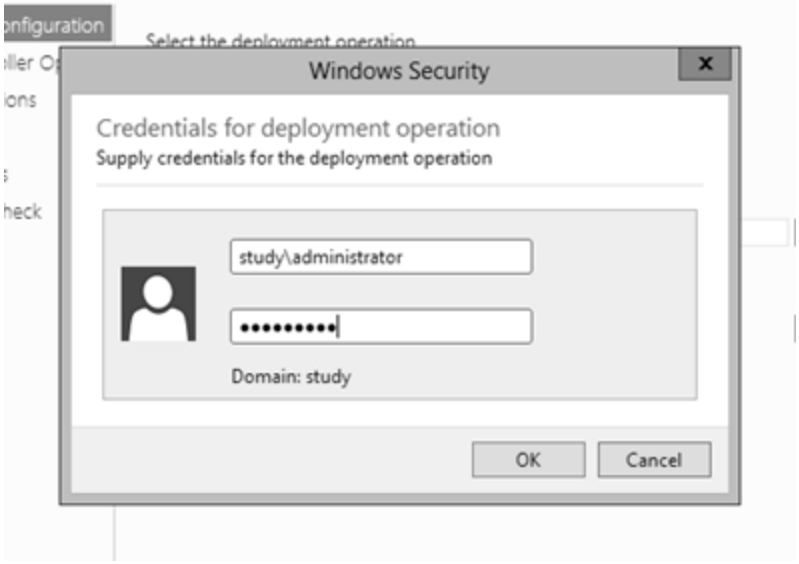


Kiedy na pasku powiadomien pojawi się wykrzyknij, trzeba kliknąć na niego, a później na Promote this Server to a domain contro ller.

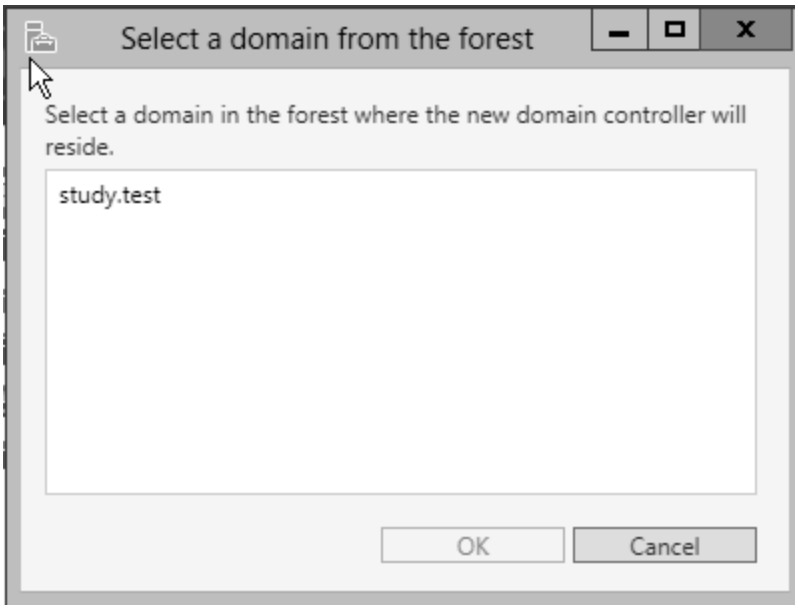
Kolejnym krokiem jest zaznaczenie Add a domain controller to an existing domain.



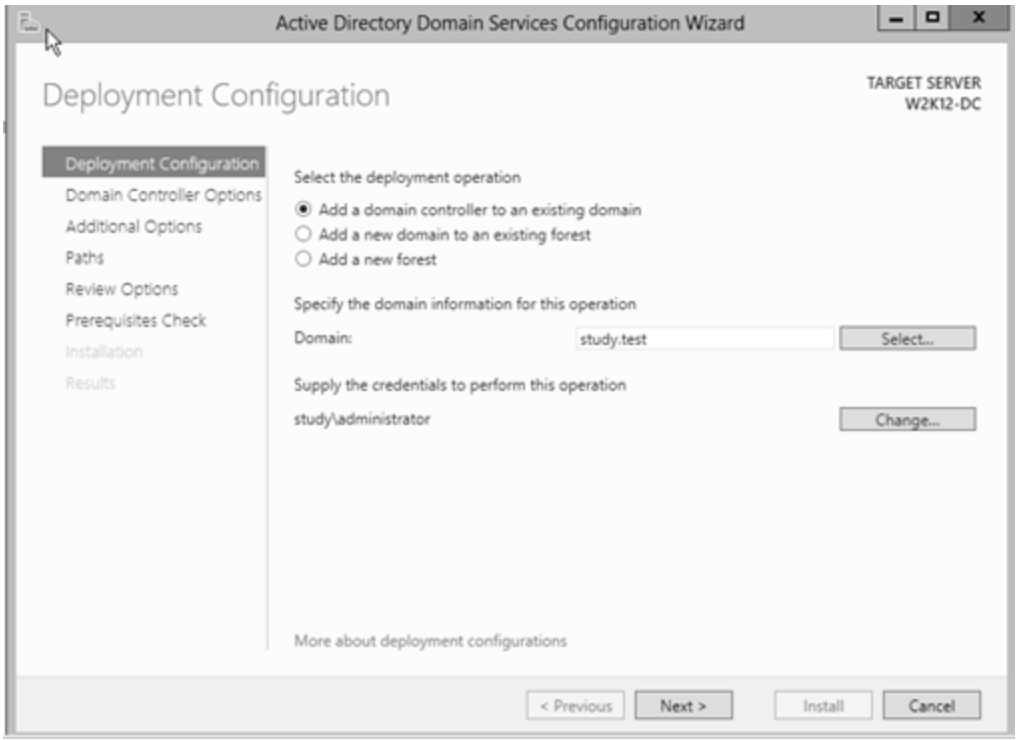
Należy kliknąć select przy specify domain information, wyskoczy okienko, w którym niezbędne będzie uzupełnienie danych Admina.



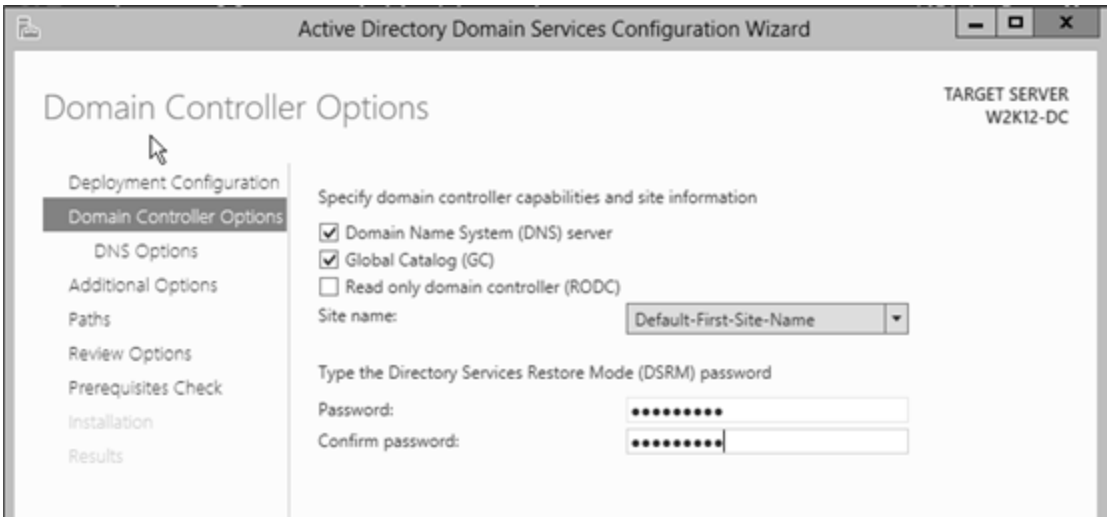
Należy zaznaczyć domenę i kliknąć OK.



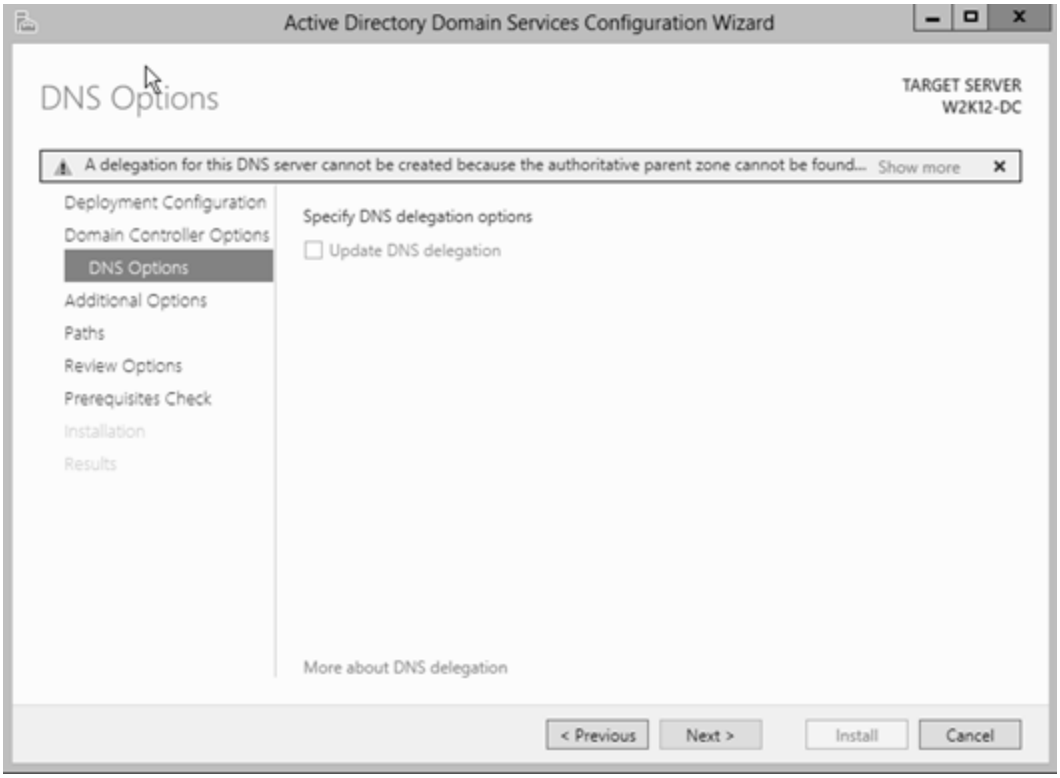
Następnie można przejść dalej, klikając Next.



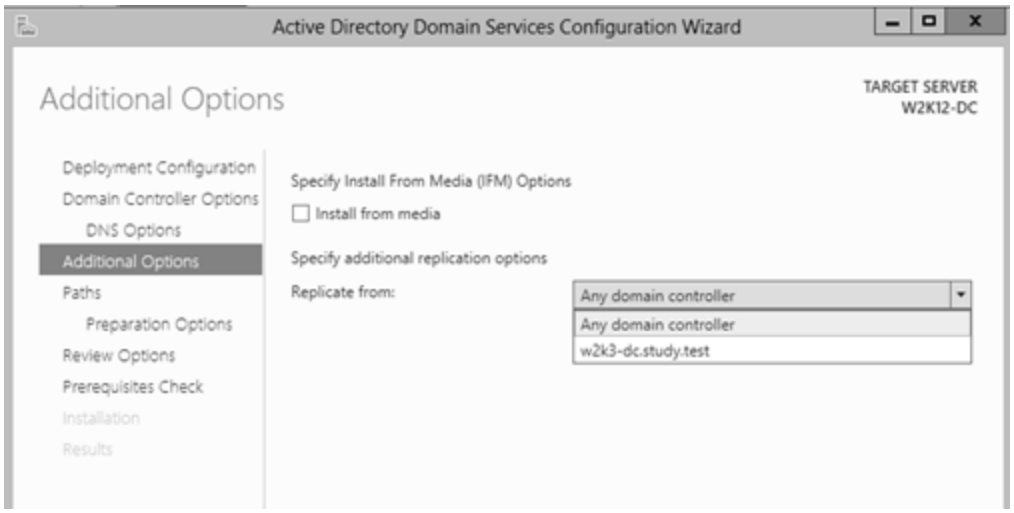
Należy teraz wybrać nazwę strony oraz wprowadzić hasło DSRM, po czym kliknąć Next.



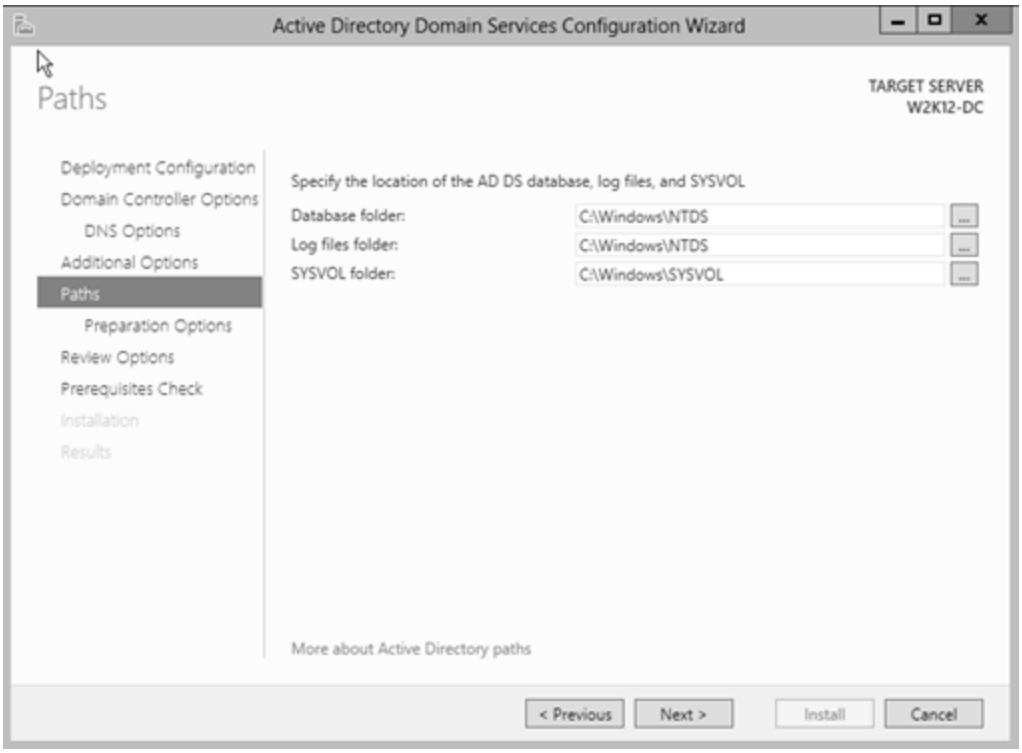
Znów należy kliknąć Next.



Teraz należy sprecyzować domenę W2K3, z której nastąpi replikacja po kliknięciu przycisku Next.

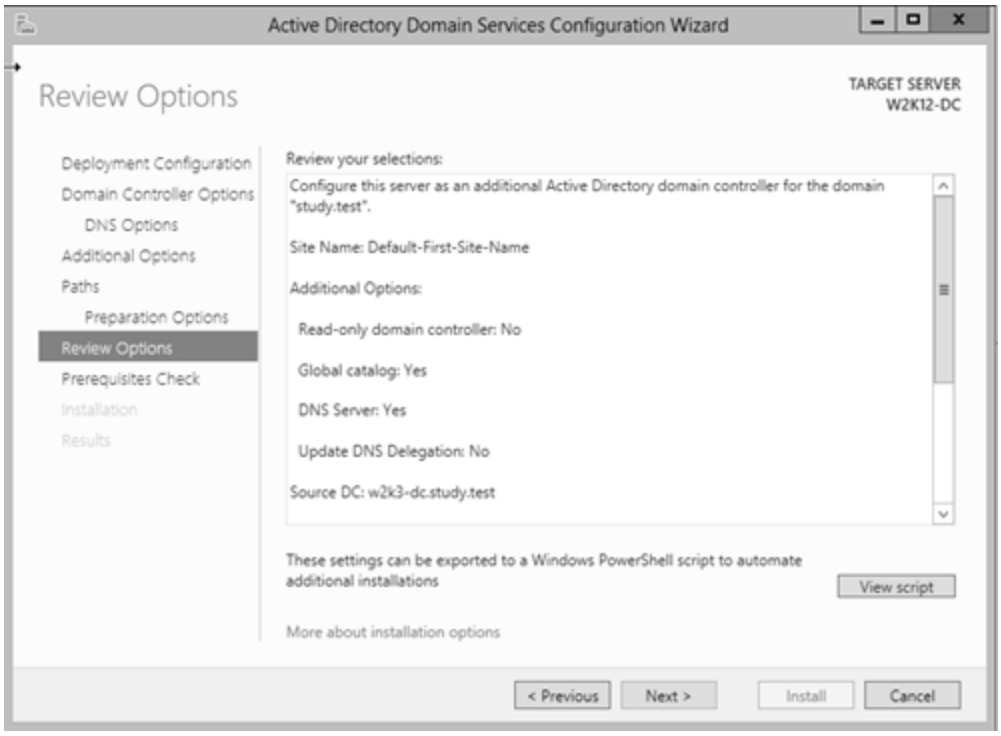


Należy wybrać database, log files i SYSVOL folder i kliknąć Next.

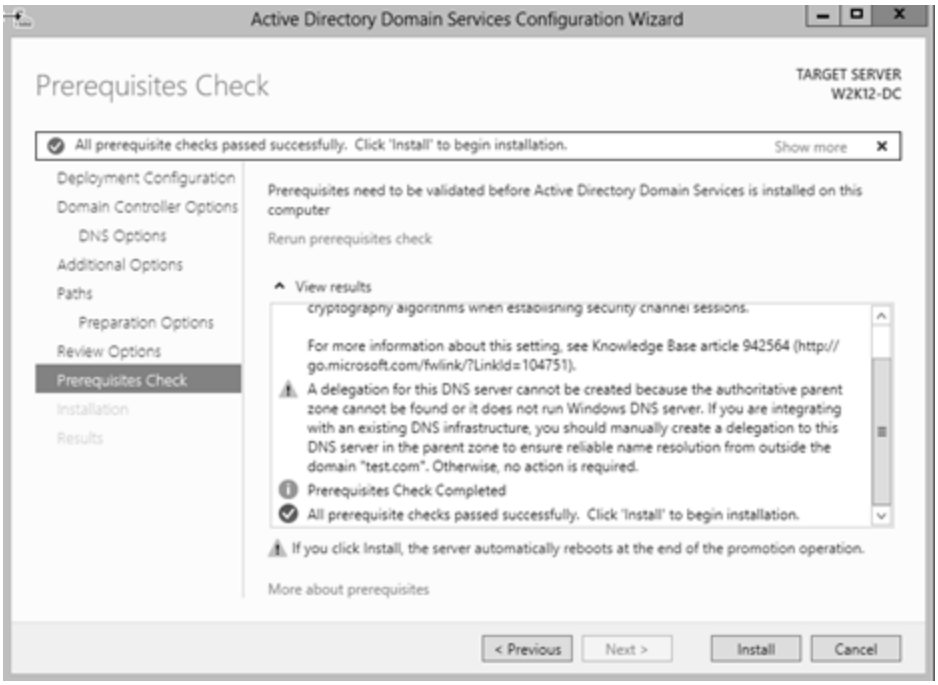


W kolejnym oknie należy kliknąć Next na preparation options, co uruchomi Adprep.

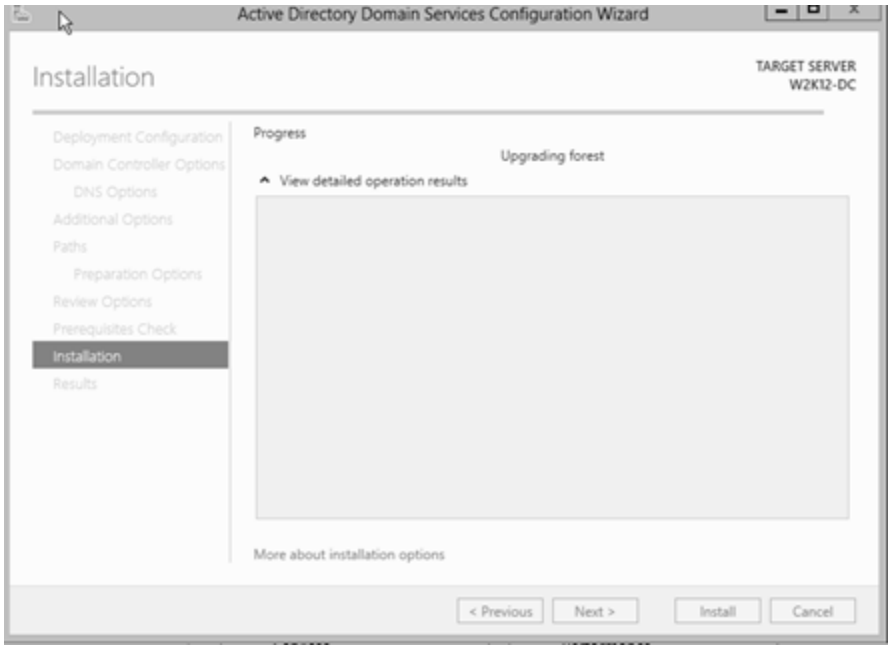
Następnie trzeba kliknąć Next na Review Options.



Gdy wszystkie wymagania wstępne są spełnione, można przejść dalej, klikając Install.



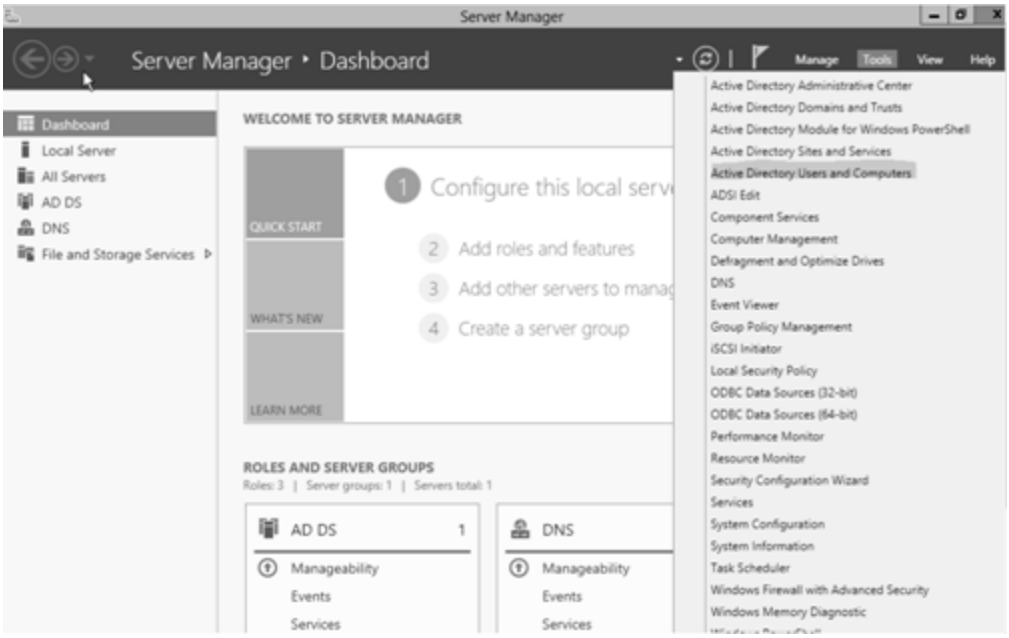
Pozostaje poczekać na postęp instalacji.



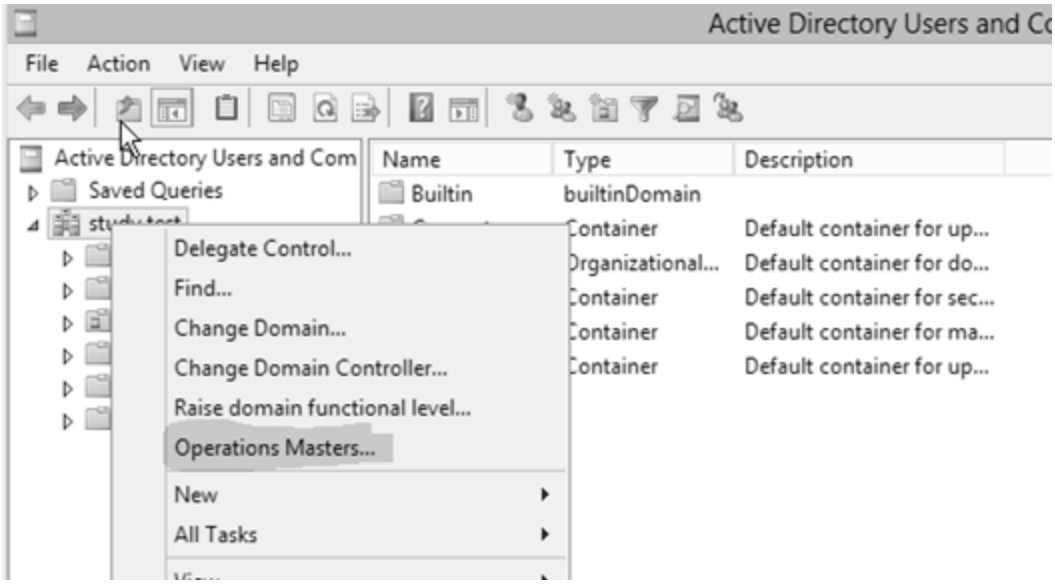
Serwer uruchomi się ponownie po ukończonej instalacji. Wówczas należy zalogować się do serwera danymi domeny.

27. Przesyłanie roli Flexible Single Master Operations (FSMO)

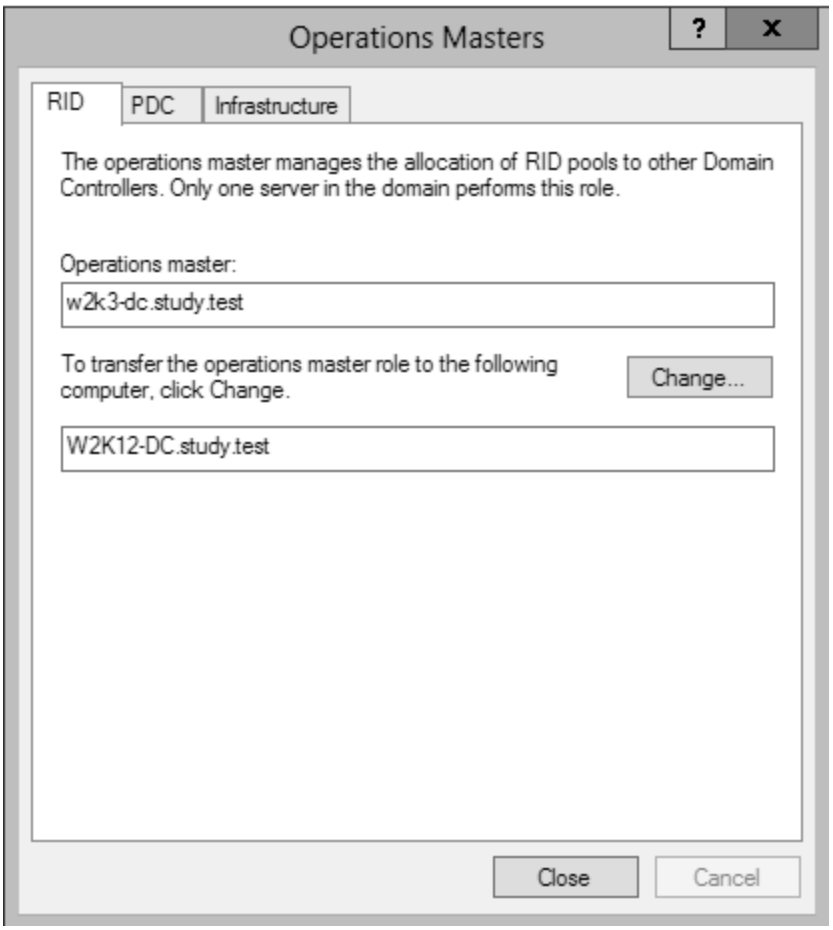
Należy przejść do Active Directory Users and Computers.



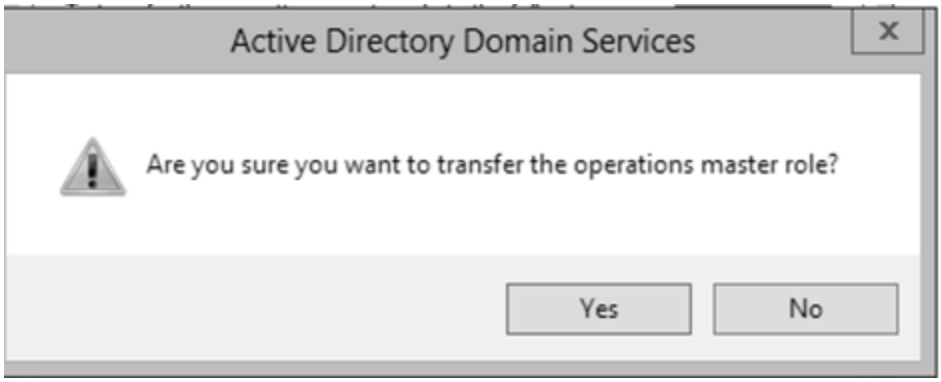
Następnie należy prejść do Operations Masters.



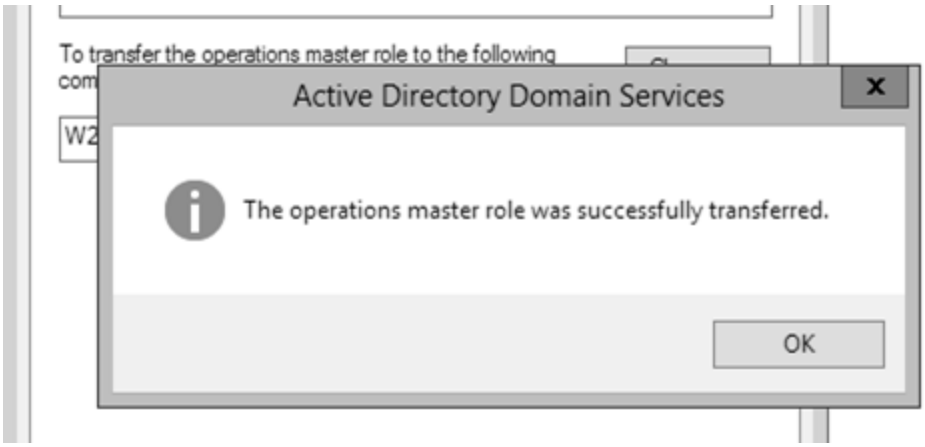
W kolejnym kroku należy przejść do zakładki RID i kliknąć Change.



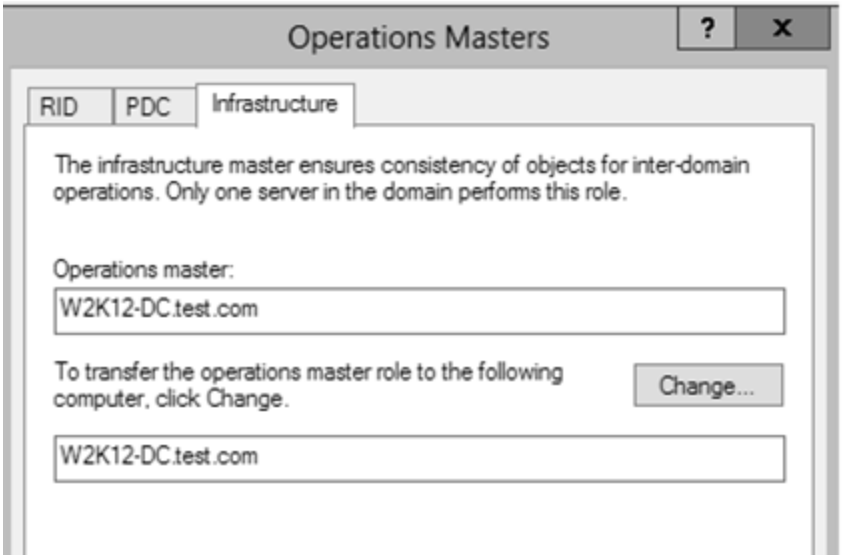
Należy kliknąć Yes.



Następnie trzeba kliknąć OK, aby potwierdzić.

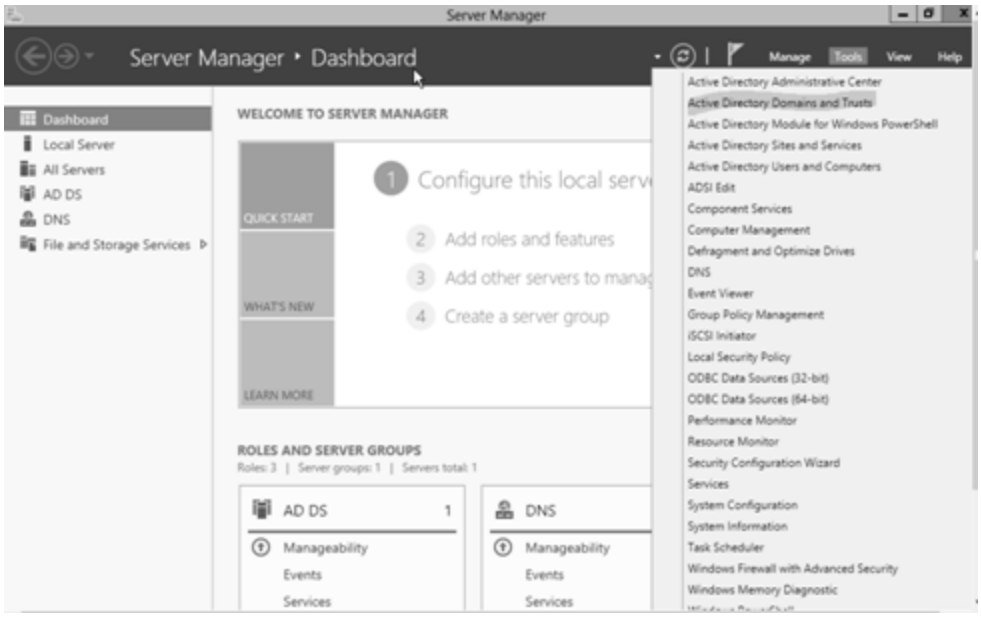


W następnej kolejności należy wykonać te same kroki dla PID and Infrastructure tabs, po czym zamknąć okno Operations Masters.

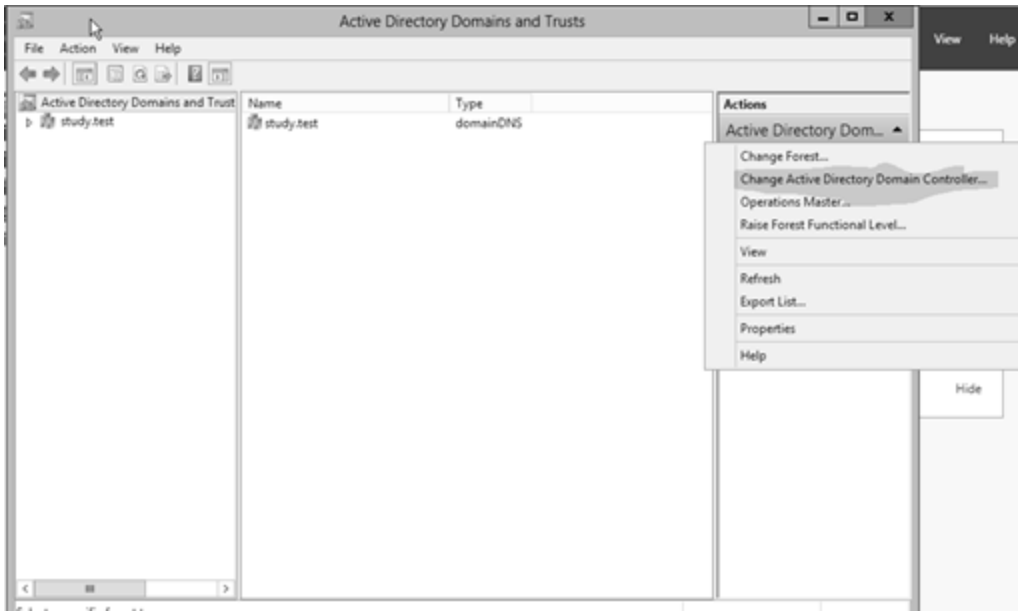


28. Zmiana Active Directory Domain Controller

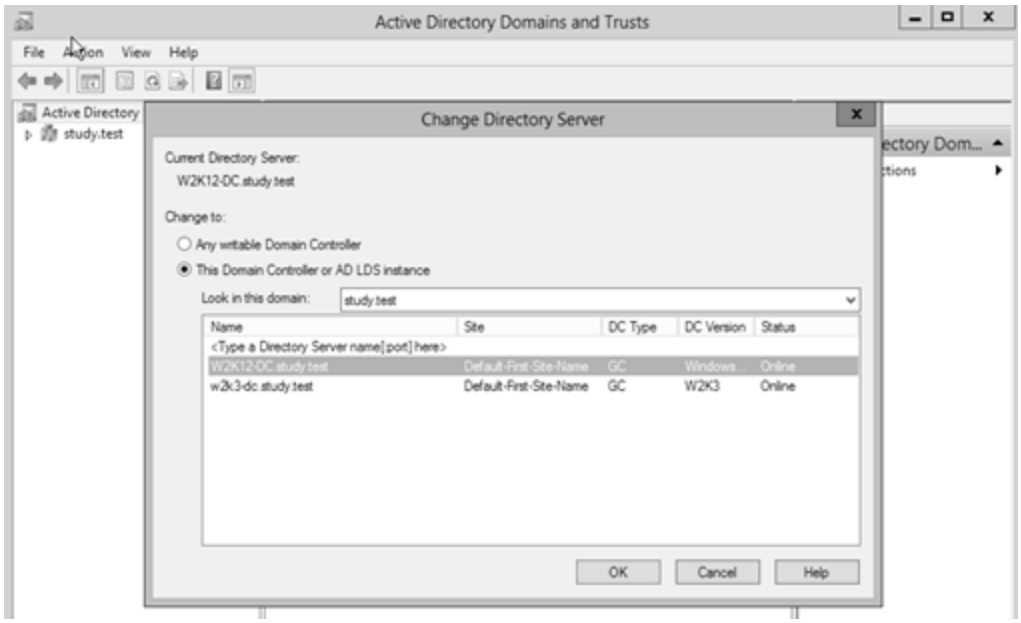
Należy przejść do Active Directory Domains and Trusts.



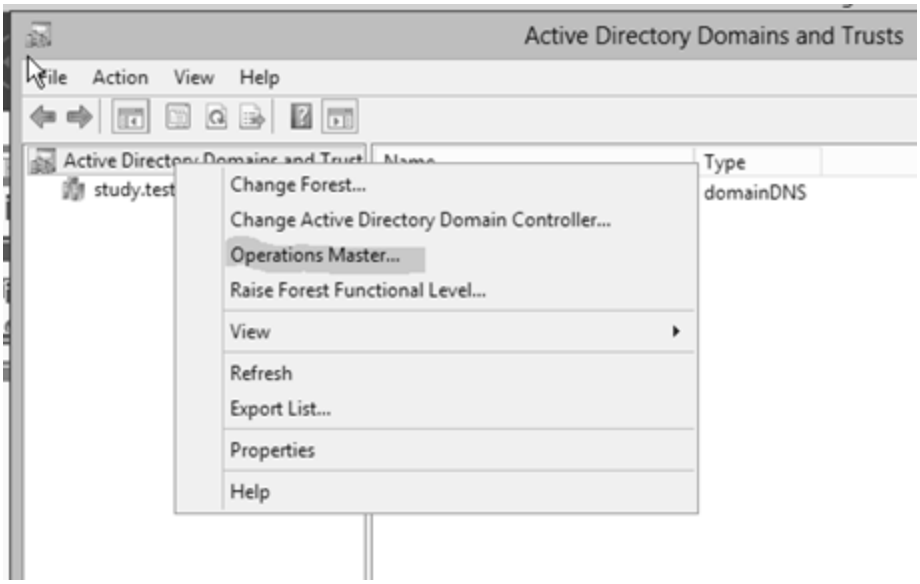
Następnie trzeba klinąć More Actions i wybrać Change Active Directory Domain Controller.



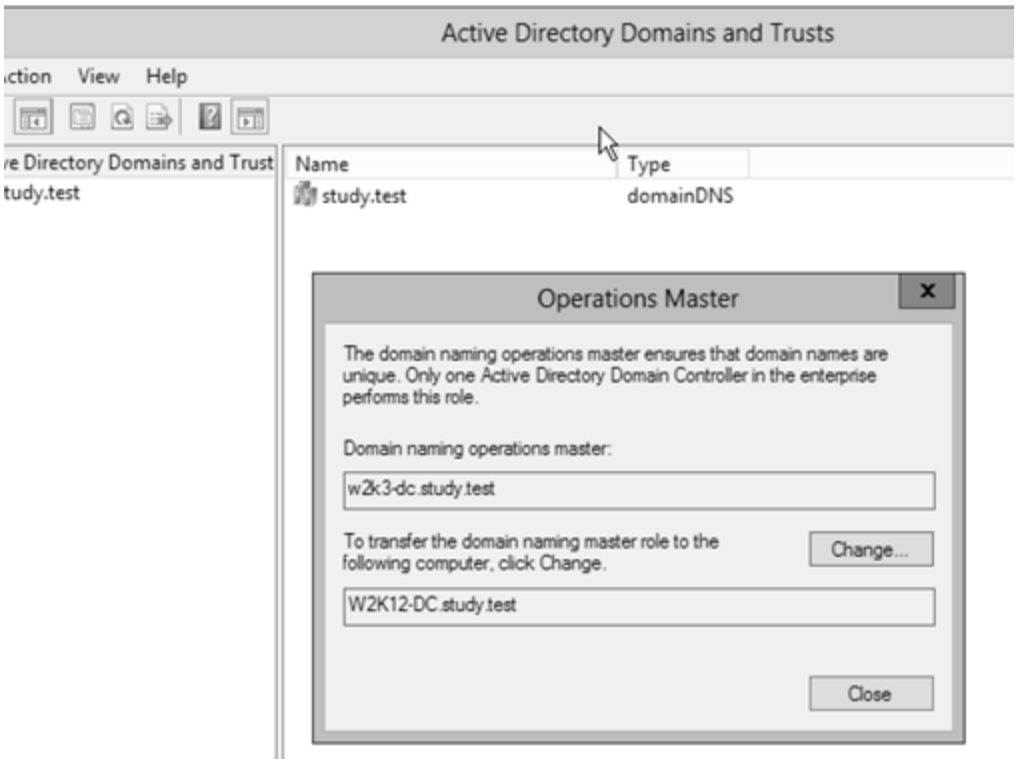
W oknie Change Directory Server, należy wybrać This Domain Controller lub AD LDS instance. Następnie trzeba wybrać New Windows 2012 Server i kliknąć OK.



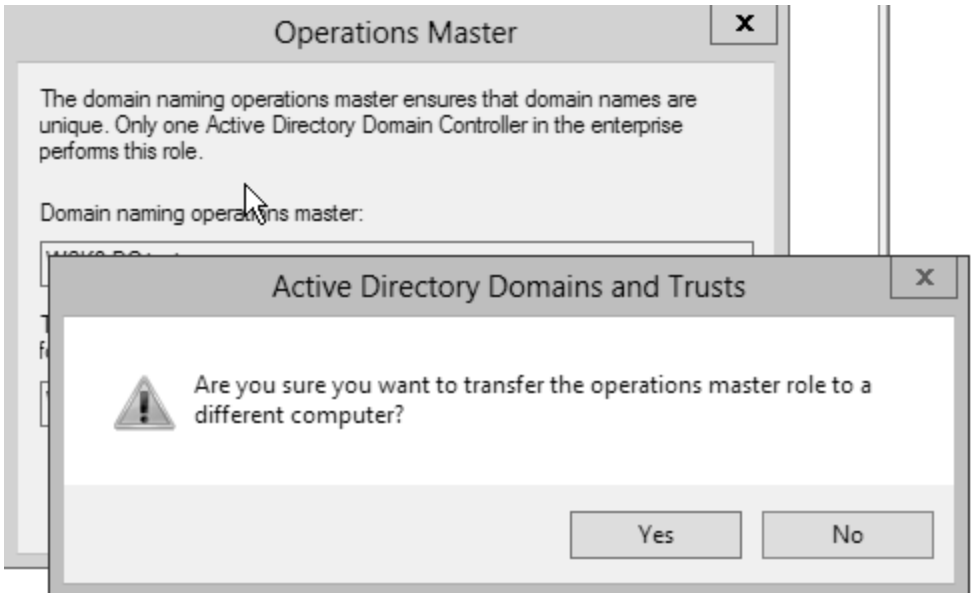
Po kliknięciu prawym przyciskiem myszy na Active Directory Domains and Trusts, należy wybrać Operations Masters.



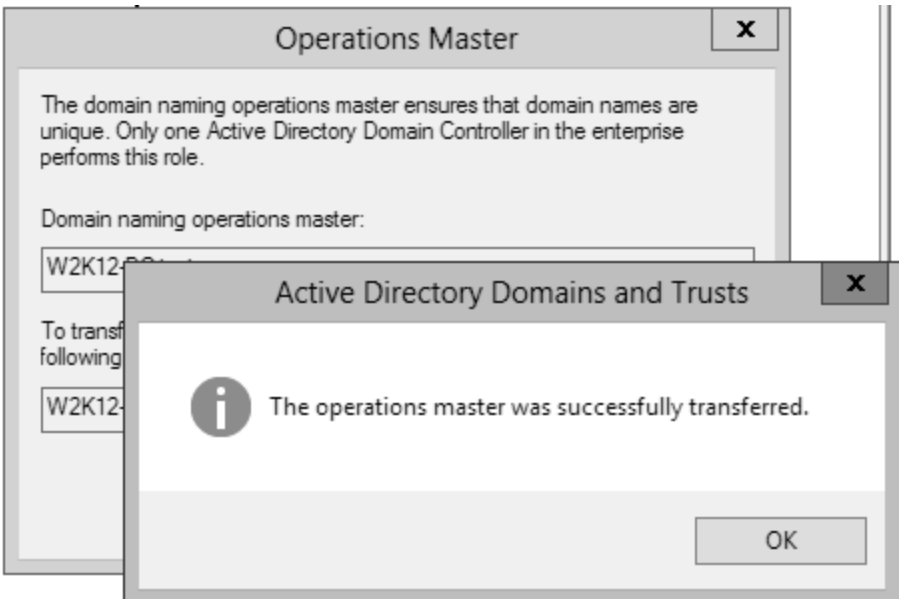
Następnie należy kliknąć Change w oknie Operations Master.



Aby potwierdzić, należy kliknąć Yes.



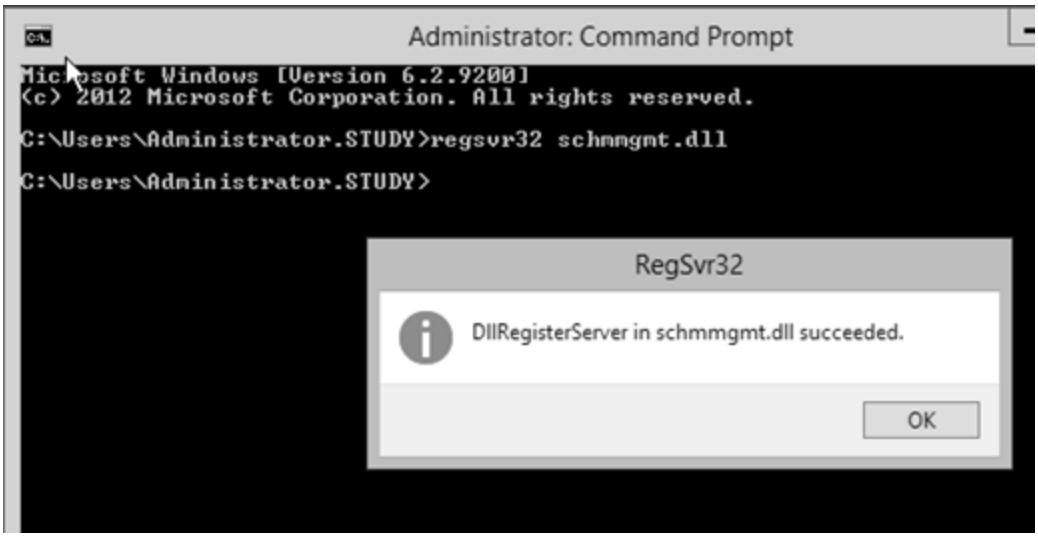
Aby przejść dalej, trzeba kliknąć Ok.



Na koniec należy zamknąć okna Operations Master i Active Directory Domains and Trusts.

29. Zmiana schematu wzorcowego

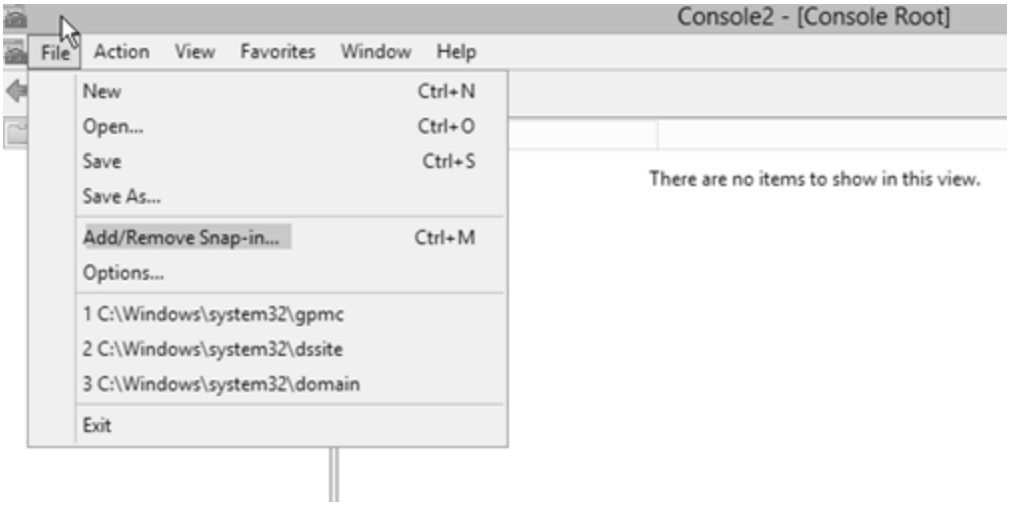
Należy otworzyć CMD i wpisać regsvr32 schmmgmt.dll.



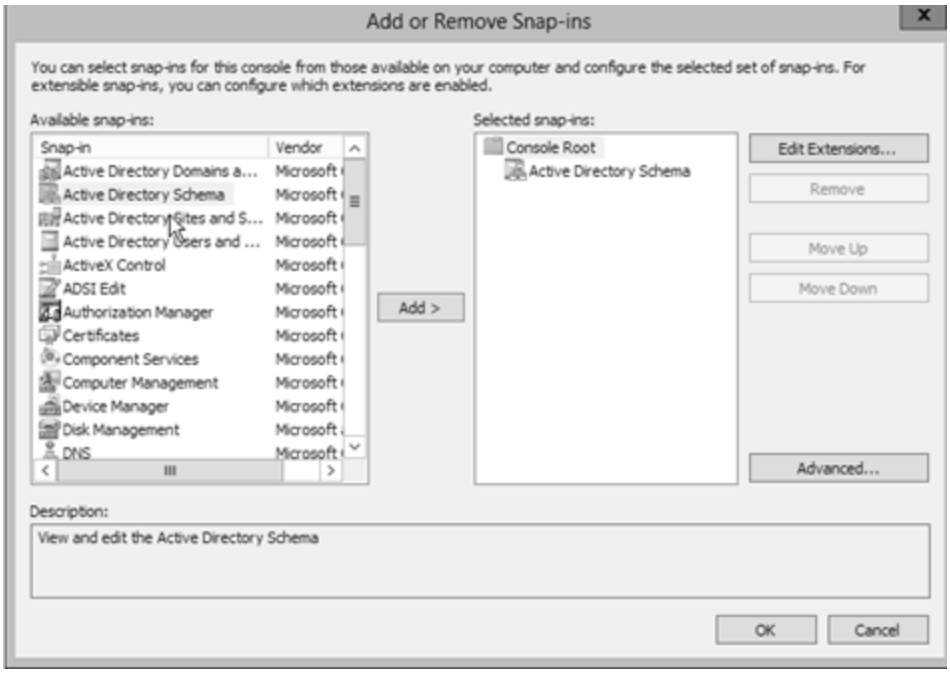
Następnie należy zamknąć CMD.

30. Dodawanie konsoli schematu Active Directory z MMC

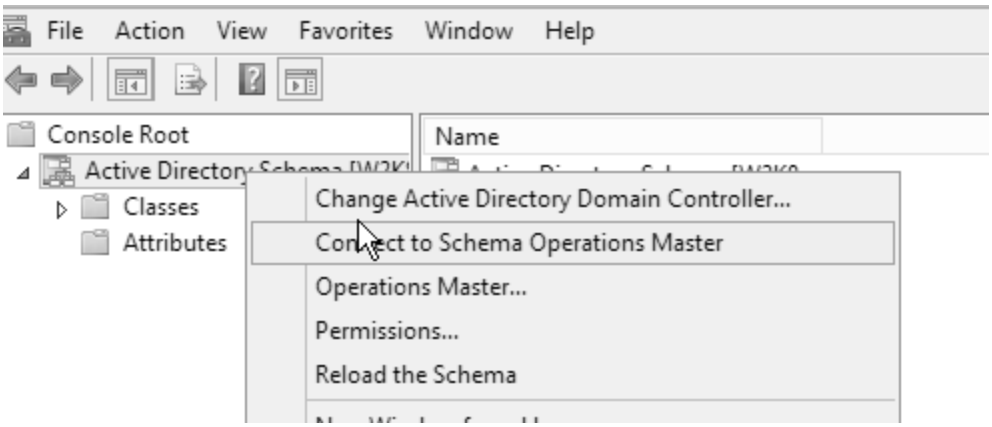
Należy otworzyć MMC, a następnie kliknąć Add/Remove Snap-in.



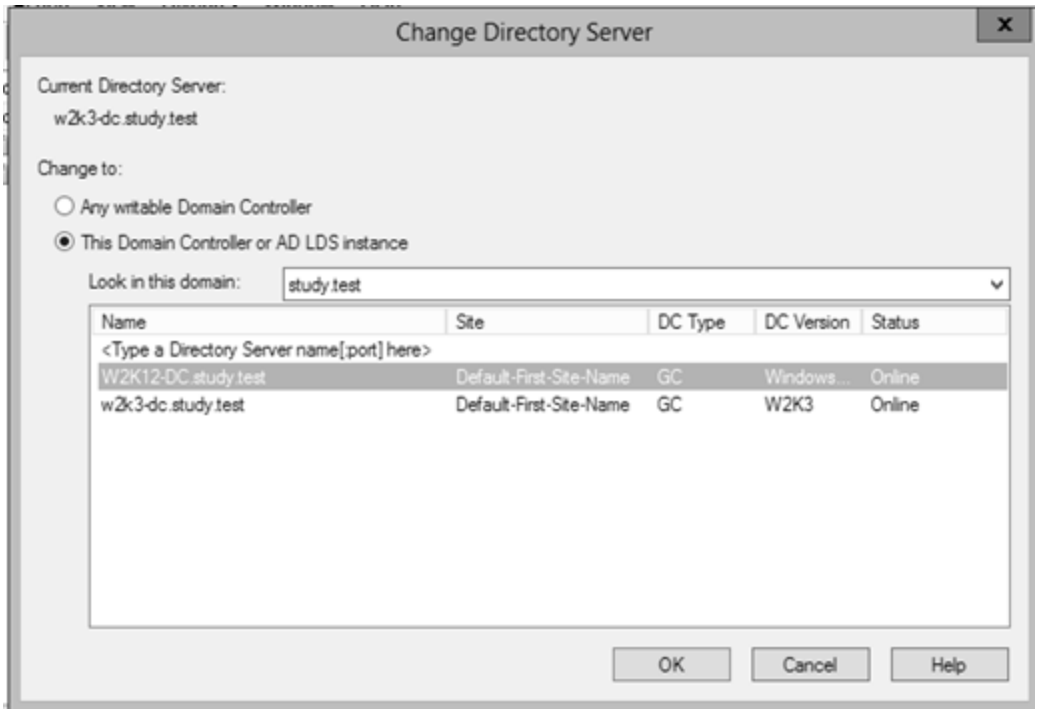
Aby przejść dalej trzeba kliknąć Active Directory Schema -> Add i dalej OK.



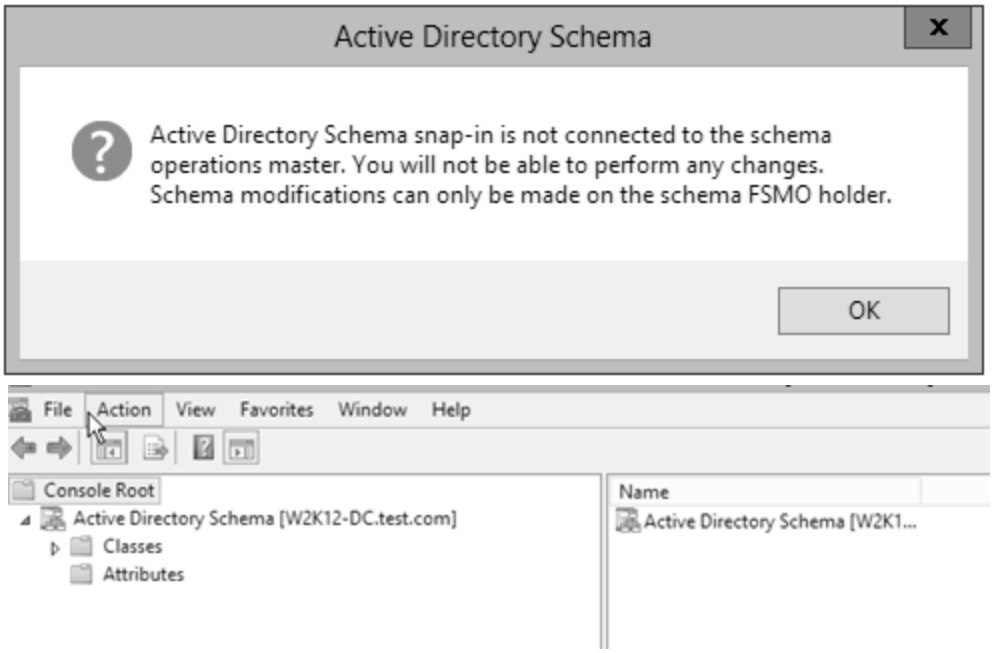
Należy nacisnąć prawym przyciskiem myszy na Active Directory Schema i kliknąć Change Active Domain Controller.



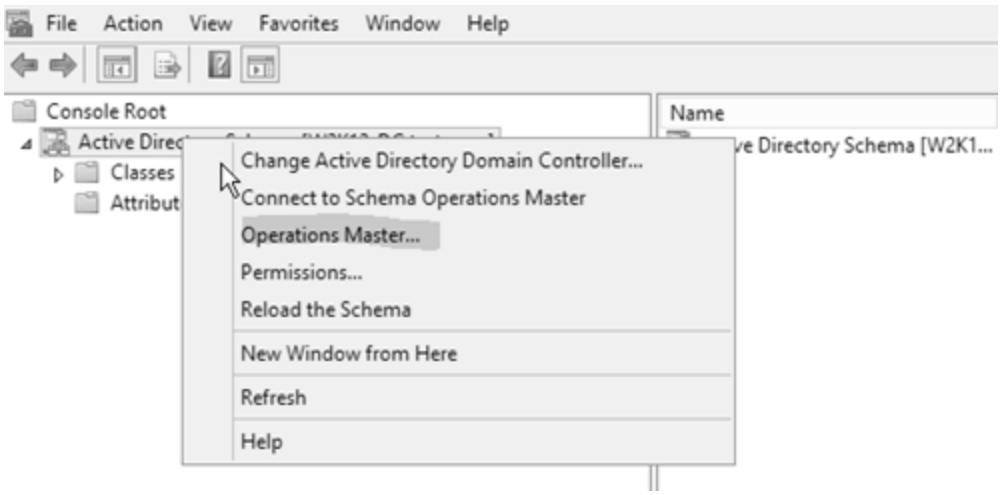
Następnie należy wybrać This Domain Controller lub instancję AD LDS i wybrać new windows 2012 server i kliknąć OK.



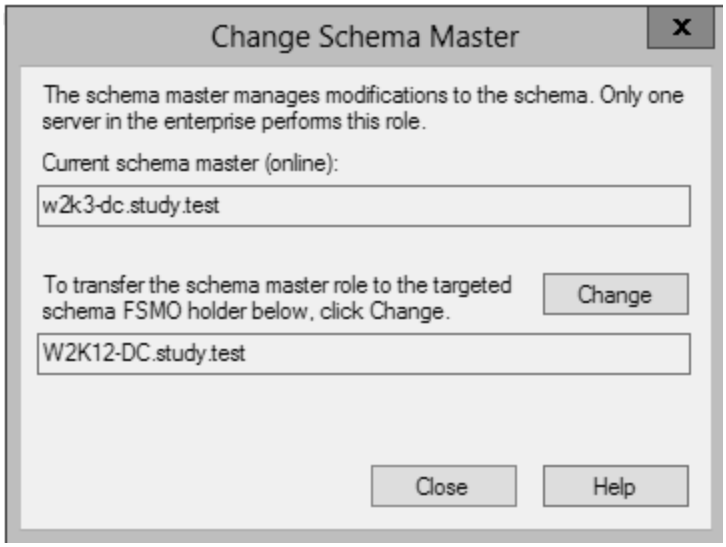
Następnie należy kliknąć OK.



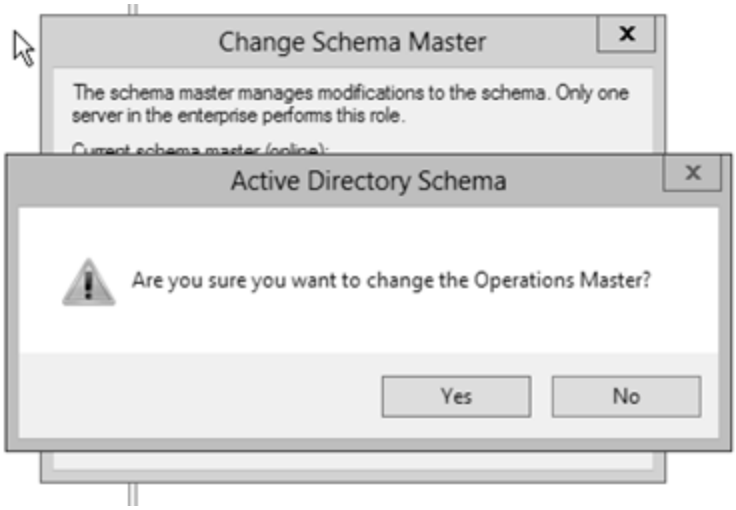
Aby przejść dalej, należy kliknąć prawym przyciskiem myszy na Active Directory Schema i wybrać Operations Master.



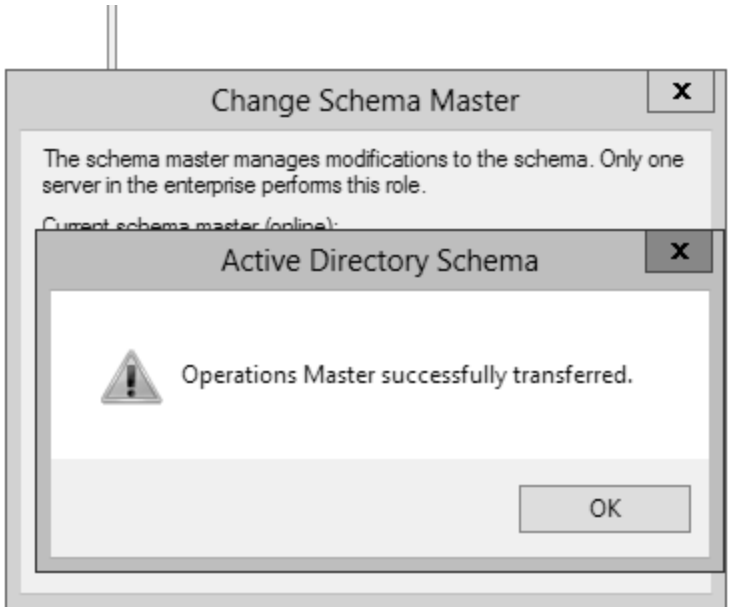
W oknie Change Schema Master, należy kliknąć Change.



Następnie należy kliknąć Yes.



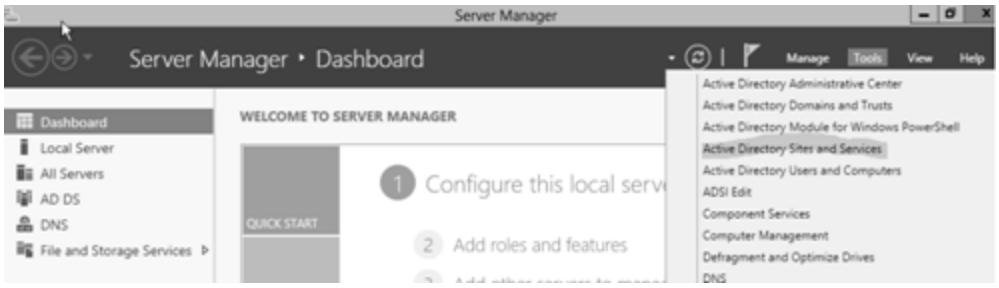
I zatwierdzić przyciskiem OK.



Należy zamknąć Change schema Master i MMC, nie zapisując MMC.

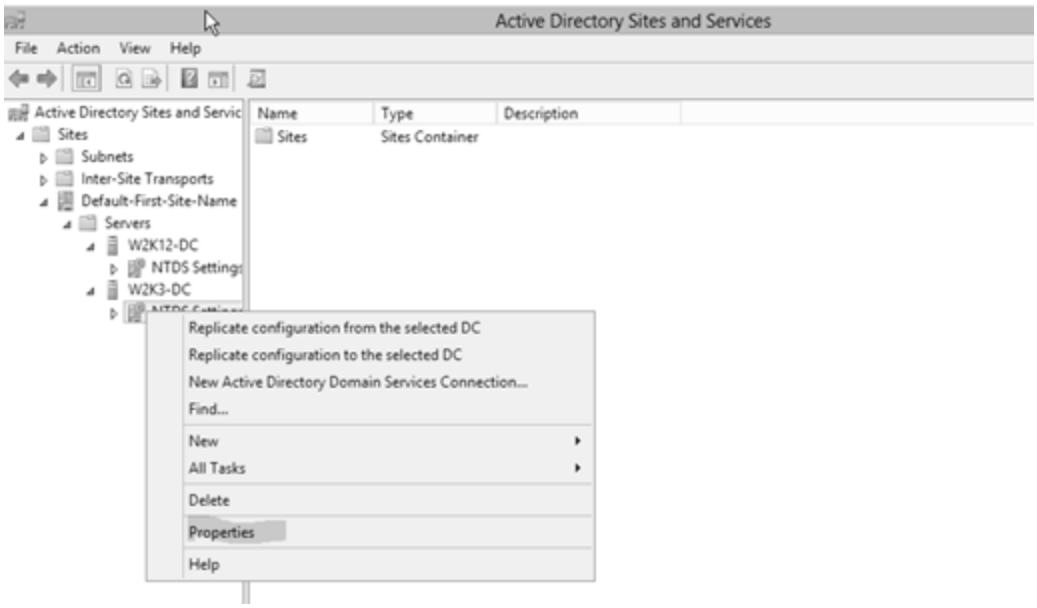
31. Usuwanie serwera z głównego katalogu.

Należy przejść do Active Directory Sites and Services.

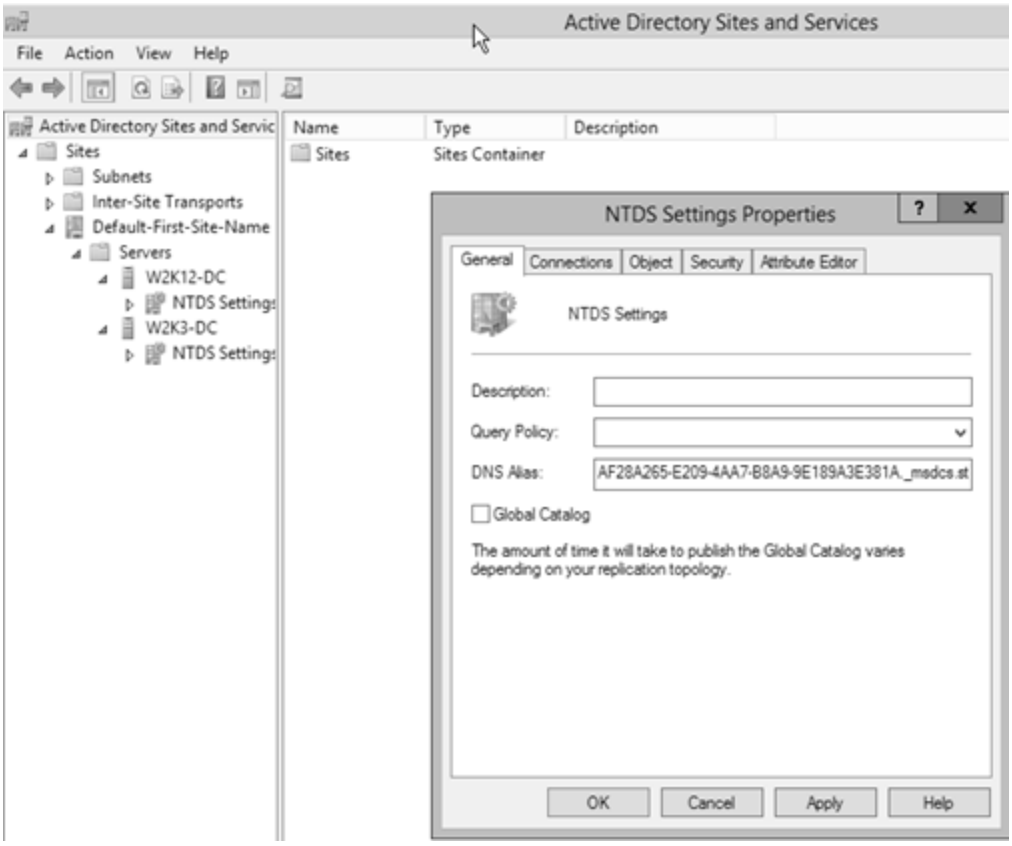


Następnie rozwinąć folder Sites. Dalej rozwinąć folder Default-First-Site-Name, a później folder Server. W kolejnym kroku należy rozwinąć oba serwery, po czym

kliknąć prawym przyciskiem myszy na NTDS Settings pod old Windows 2008 DC i i dalej kliknąć properties.



Zanim można przejść dalej, należy odznaczyć pole Global Catalog.



Dalej trzeba kliknąć OK i zamknąć Active Directory Sites and Services.

32. Migracja z Windows Server 2008

Wymagania wstępne:

1. Należy się upewnić, że oba serwery są zaktualizowane do najnowszej wersji Service Pack.

2. Należy się upewnić, że serwer Windows 2008 jest na poprawnym poziomie funkcjonalnym.

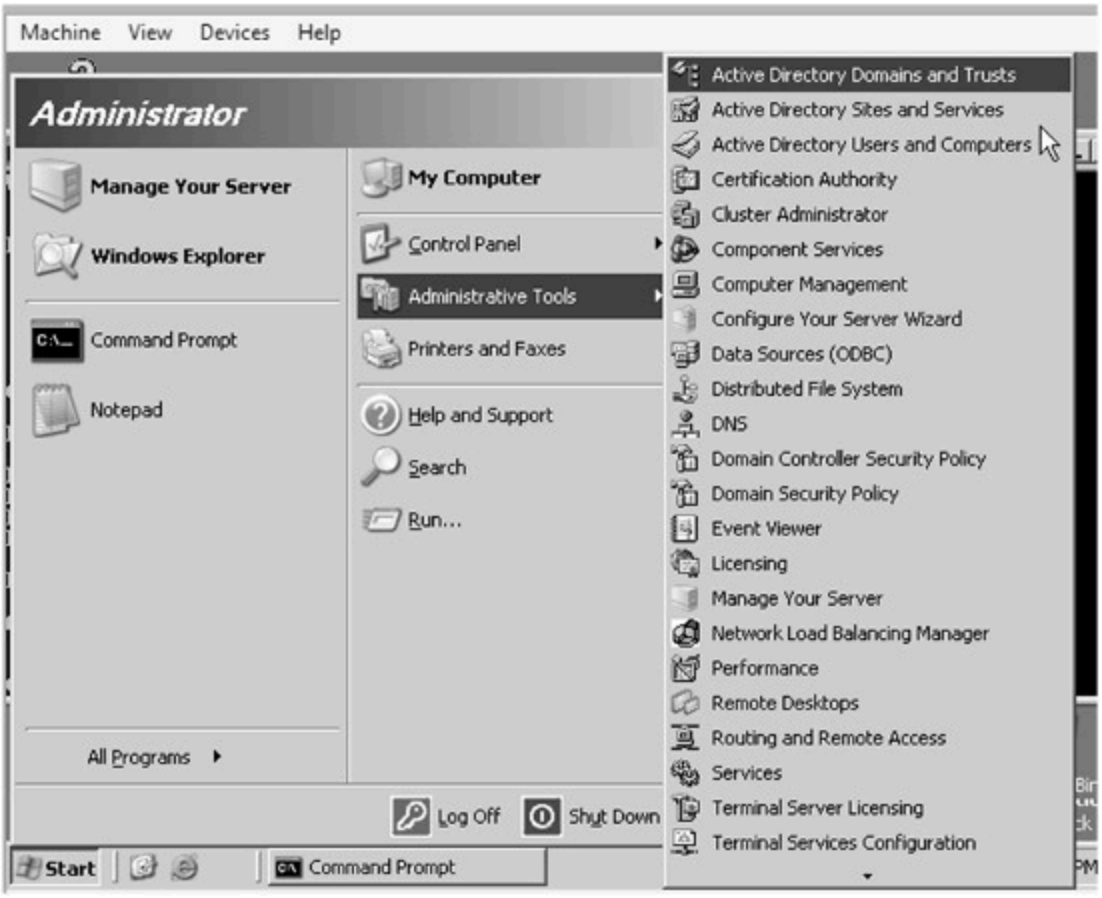
3. Jeżeli nie jest, należy podnieść poziom domeny do Windows Server 2008.

4. Poziom domeny nie musi być podniesiony w przypadku, gdy jest prawidłowy.

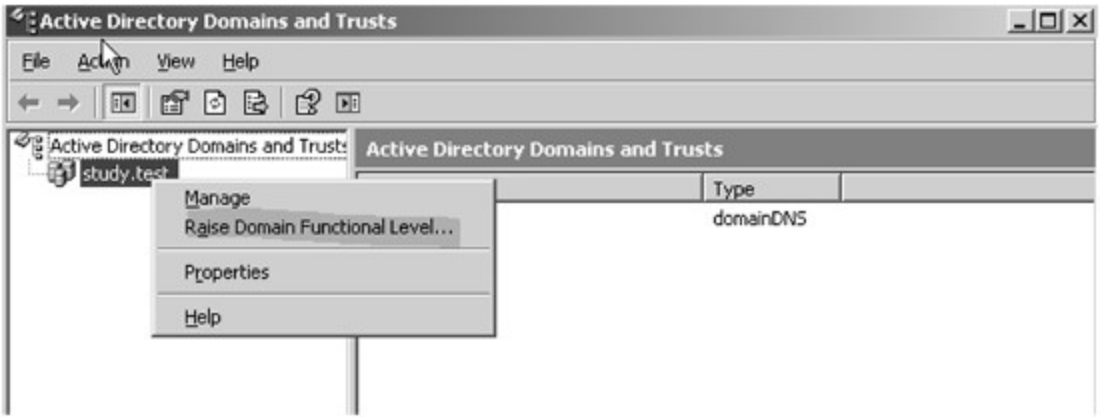
5. Należy się upewnić, że jesteśmy członkiem Enterprise Admins Group w AD.

32.1. Podnoszenie Domain Functional Level

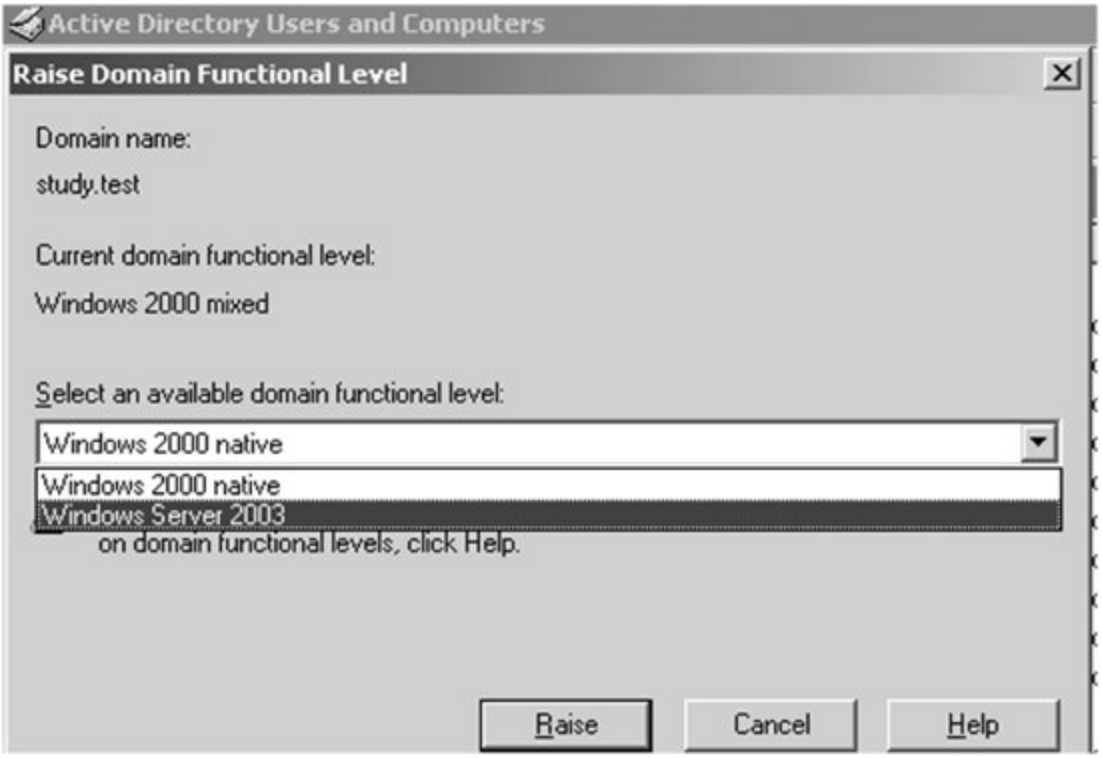
Należy przejść do Active Directory Domains and Trusts.



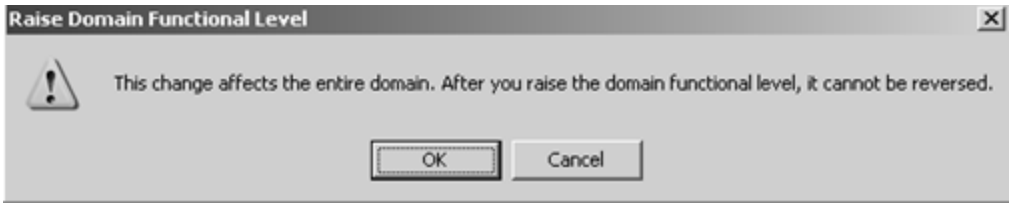
Następnie należy kliknąć prawym przyciskiem myszy na kontrolerze domeny i dalej kliknąć Raise Domain Functional Level.



Należy wybrać Domain Functional Level jako Windows Server 2008.



Następnie należy kliknąć Raise i potwierdzić przyciskiem OK.

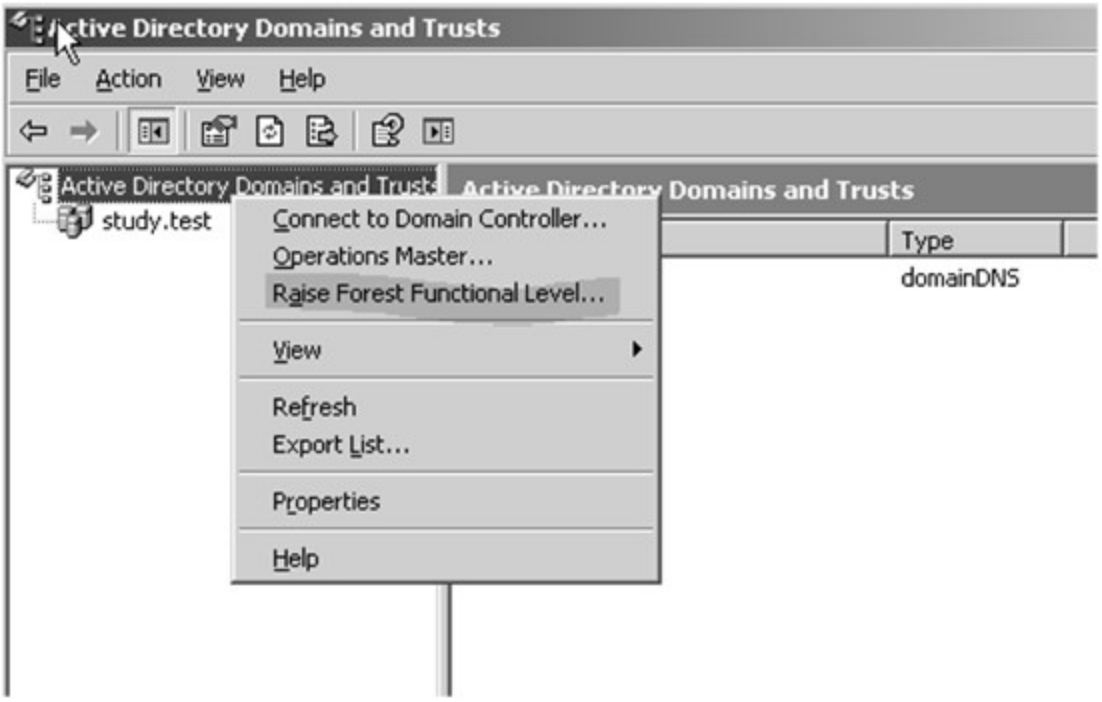


Ponownie należy kliknąć OK.

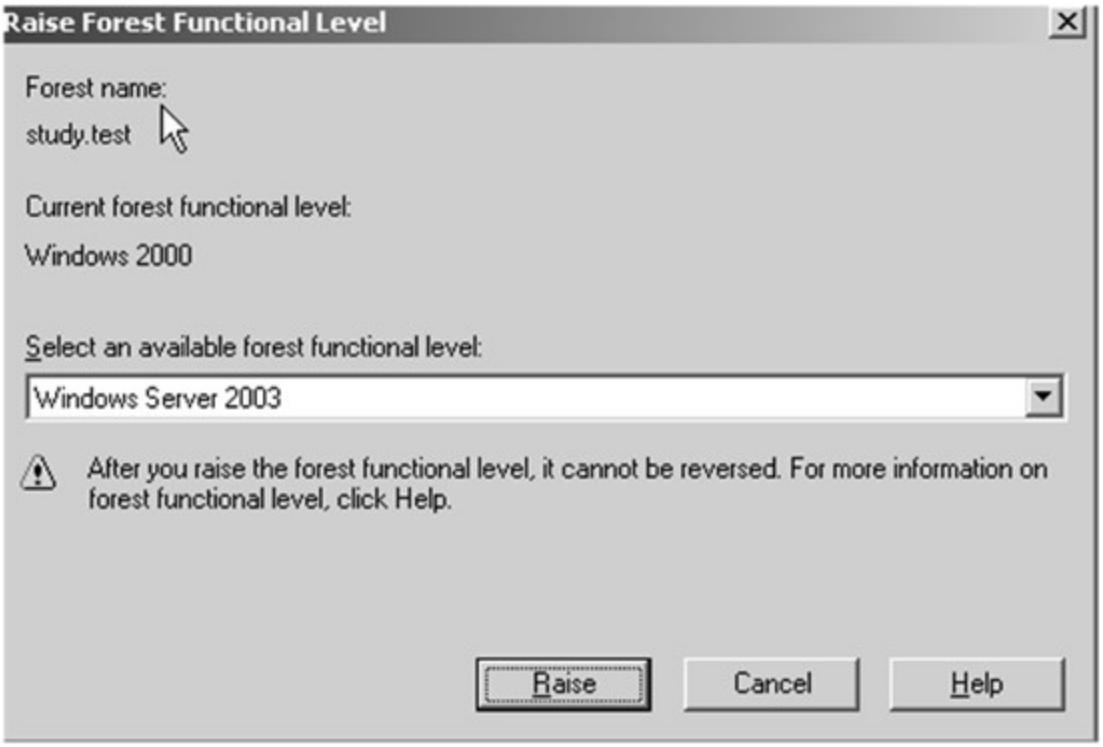
Można kliknąć prawym przyciskiem myszy na kontrolerze domeny, po czym kliknąć na Raise Domain Controller, aby potwierdzić poziom domeny. Teraz jest on na Windows Server 2008.

Należy nacisnąć prawym przyciskiem myszy na Active Directory Domains and Trusts, po czym kliknąć Raise Forest

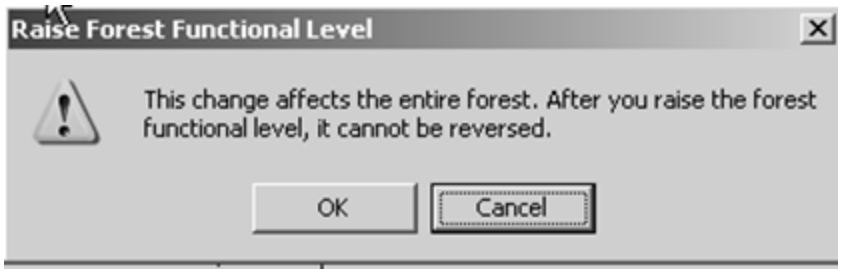
functional Level.



Należy wybrać Windows 2008 i kliknąć Raise.



Aby potwierdzić, należy kliknąć OK.



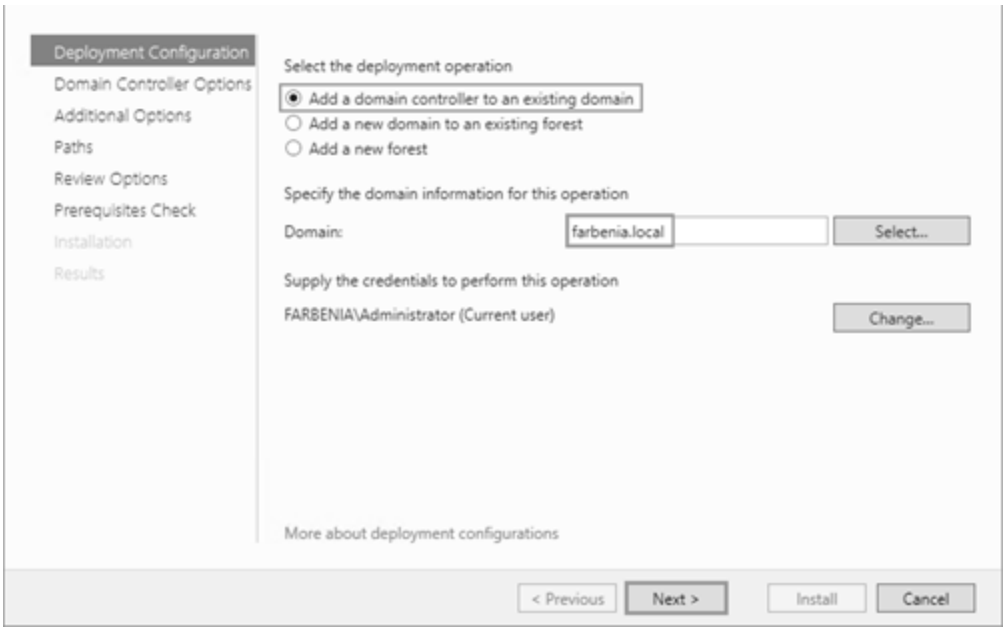
I ponownie należy kliknąć OK.

33. Migracja z Windows 2012

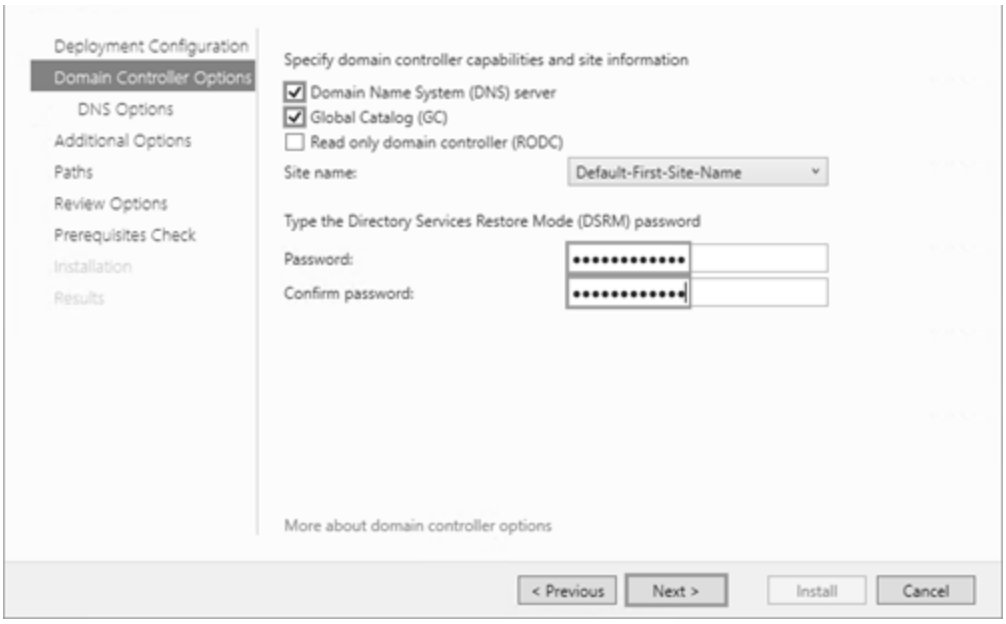
Prace związane z migracją usługi katalogowej Active Directory trzeba rozpocząć od instalacji systemu operacyjnego Windows Server 2016 Standard – proces instalacji jest bardzo prosty, w związku z tym ten krok zostanie pominięty. Po wykonaniu instalacji należy upewnić się, że zostały zainstalowane najnowsze aktualizacje, przypisany statyczny adres IP (w tym przypadku 192.168.0.101) oraz wprowadzona została poprawnie nazwa dla kontrolera domeny (w tym przypadku będzie to dc2016), serwer należy podpiąć do bieżącej domeny.

Gdy zostaną wykonane wszystkie wyżej opisane czynności, można przejść do dodania roli. W tym celu, w poziomu Server Managera, należy wybrać opcję Add Roles and Features. Następnie w oknie kreatora należy wybrać rolę Active Directory Domain Services, dodatkowo automatycznie zostaną zaznaczone narzędzia administracyjne do zarządzania AD DS. i DNS Server. Po przeprowadzeniu instalacji roli Active Directory Domain Services należy wypromować nasz serwer do kontrolera domeny. Z poziomu Server Managera, po wykonaniu instalacji, pojawi się opcja Post-deployment Configuration – Promote this server to a domain controler, którą należy wybrać.

W kreatorze Active Directory Domain Services Configuration Wizard w kroku Deployment Configuration należy wybrać opcję Add a domain controller to an existing domain. W polu Domain trzeba upewnić się, że widnieje nazwa naszej domeny: farbenia.local.



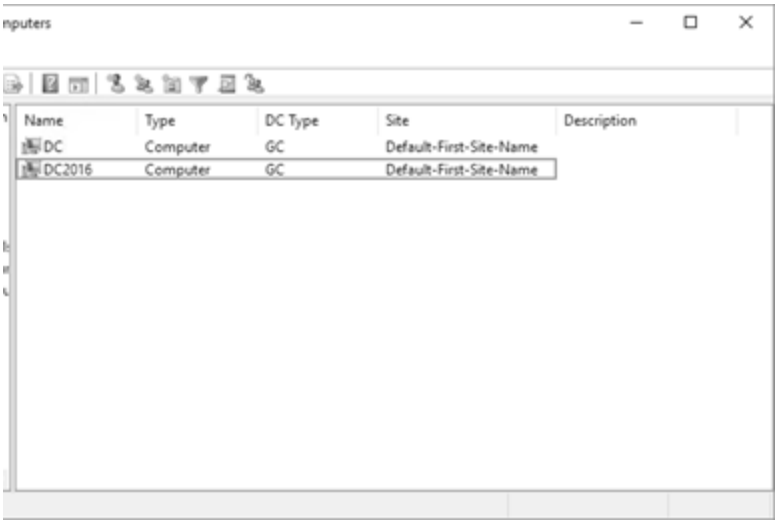
W kroku Domain Controller Options należy zaznaczyć opcję Domain Name System (DNS) server oraz Global Catalog (GC). W polu Password i Confirm Password należy wprowadzić hasło do odzyskiwania usług katalogowych Active Directory.



Pozostałe kroki: DNS Options, Additional Options, Paths itd. należy zostawić domyślnie i na końcu kreatora

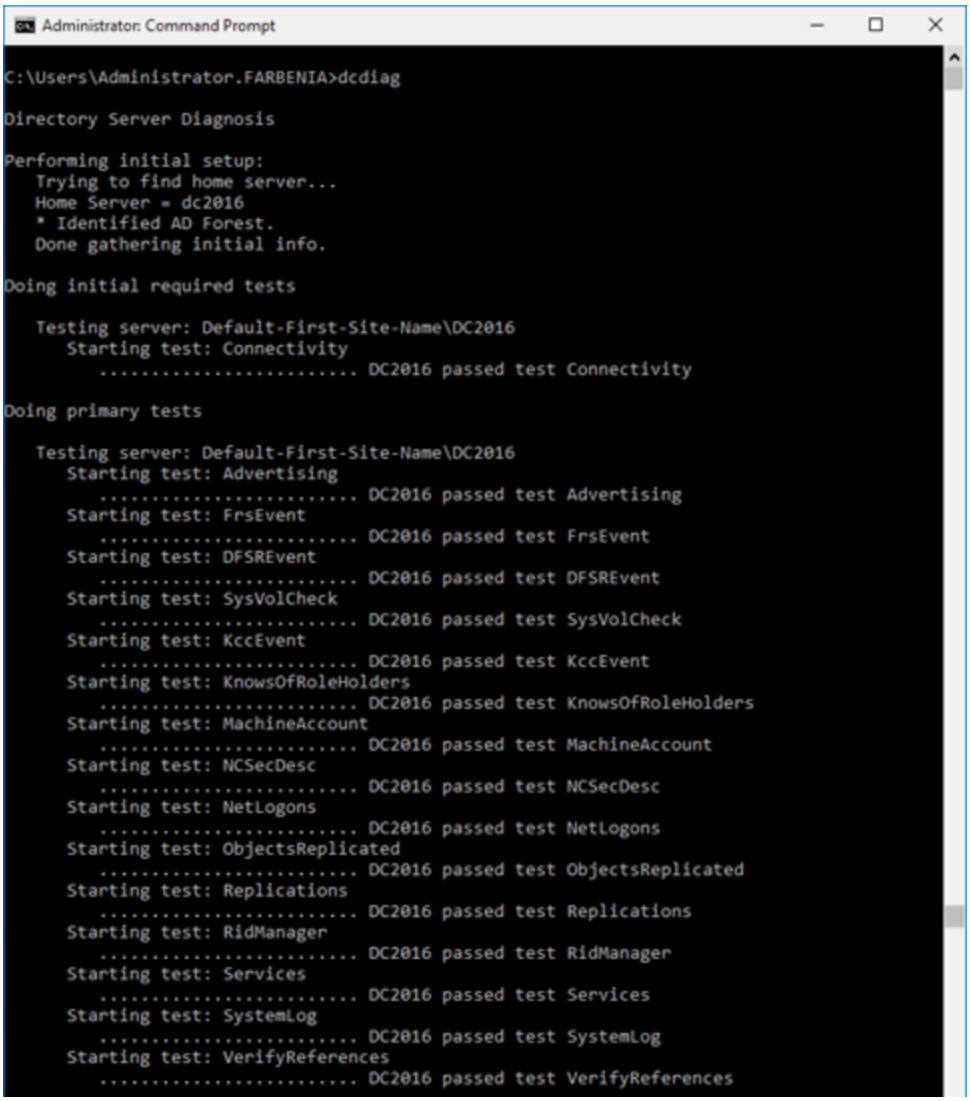
zaakceptować konfigurację za pomocą przycisku Install, który rozpocznie proces promowania nowego kontrolera domeny w domenie farbenia.local.

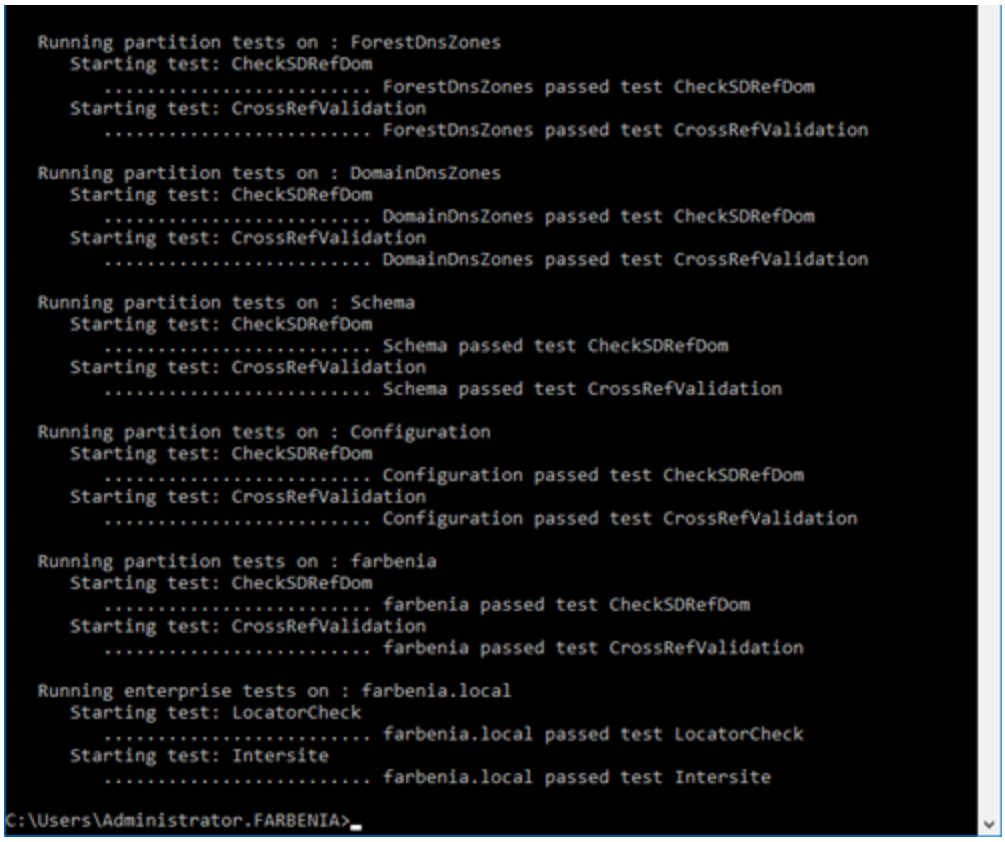
Po poprawnie przeprowadzonych czynnościach można uruchomić narzędzie Active Directory Users and Computers, przejść do jednostki organizacyjnej Domain Controllers i sprawdzić, czy pojawił się nowy kontroler domeny dc2016 (zrzut ekranu poniżej)



34. Weryfikacja poprawności działania usługi katalogowej Active Directory

Weryfikację poprawności działania domeny należy zacząć od kluczowego polecenia dcdiag, które sprawdza aktualny stan kontrolerów domeny i raportuje swoje wyniki w wierszu poleceń. Wynik komendy dcdiag został przedstawiony na zrzucie z ekranu poniżej.


Administrator: Command Prompt
C:\Users\Administrator.FARBENIA>dcdiag
Directory Server Diagnosis
Performing initial setup:
Trying to find home server...
Home Server = dc2016
* Identified AD Forest.
Done gathering initial info.
Doing initial required tests
Testing server: Default-First-Site-Name\DC2016
Starting test: Connectivity
..... DC2016 passed test Connectivity
Doing primary tests
Testing server: Default-First-Site-Name\DC2016
Starting test: Advertising
..... DC2016 passed test Advertising
Starting test: FrsEvent
..... DC2016 passed test FrsEvent
Starting test: DFSREvent
..... DC2016 passed test DFSREvent
Starting test: SysVolCheck
..... DC2016 passed test SysVolCheck
Starting test: KccEvent
..... DC2016 passed test KccEvent
Starting test: KnowsOfRoleHolders
..... DC2016 passed test KnowsOfRoleHolders
Starting test: MachineAccount
..... DC2016 passed test MachineAccount
Starting test: NCSecDesc
..... DC2016 passed test NCSecDesc
Starting test: NetLogons
..... DC2016 passed test NetLogons
Starting test: ObjectsReplicated
..... DC2016 passed test ObjectsReplicated
Starting test: Replications
..... DC2016 passed test Replications
Starting test: RidManager
..... DC2016 passed test RidManager
Starting test: Services
..... DC2016 passed test Services
Starting test: SystemLog
..... DC2016 passed test SystemLog
Starting test: VerifyReferences
..... DC2016 passed test VerifyReferences



Kolejnym przydatnym narzędziem do weryfikacji replikacji pomiędzy kontrolerami domeny jest polecenie repadmin z przełącznikami /synccall oraz/showreps.

Polecenie repadmin /synccall wymusza synchronizację pomiędzy wszystkimi kontrolerami w domenie.

Polecenie repadmin /showrepl wyświetla topologię replikacji pomiędzy kontrolerami domeny oraz ich status.

35. Przeniesienie ról FSMO na nowy kontroler domeny

Przed przystąpieniem do przeniesienia ról FSMO (Flexible Single Master Operation) na nowy kontroler domeny z systemem Windows Server 2016 należy zaktualizować usługę katalogową Active Directory za pomocą poniższych poleceń:

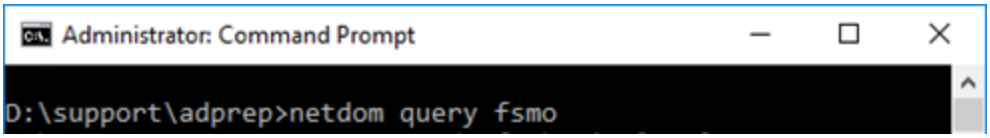
adprep /forestprep

adprep /domainprep

Narzędzie adprep znajduje się na nośniku instalacyjnym systemu Windows Server 2016 w katalogu support/adprep.

Następnie z poziomu wiersza poleceń, za pomocą polecenia netdom query fsmo, można sprawdzić, na którym serwerze aktualnie przechowywane są role FSMO. Zgodnie ze zrzutem ekranu poniżej wszystkie role znajdują się na kontrolerze domeny dc.elitepc.local:

- Schema master,
- Domain naming master,
- PDC,
- RID pool manager,
- Infrastructure master.

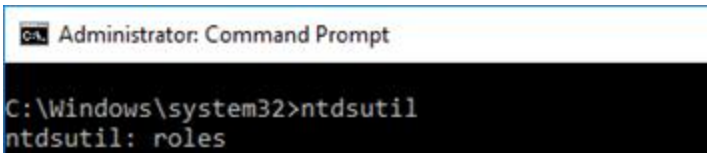


Role FSMO można przenieść za pomocą interfejsu graficznego lub za pomocą narzędzia ntdsutil z poziomu wiersza poleceń. Ja osobiście od jakiegoś czasu jestem fanem wiersza poleceń, między innymi z prostoty dokumentacji wykonywanych czynności.

Z poziomu wiersza poleceń należy uruchomić narzędzie ntdsutil (zrzut ekranu poniżej) Gdzie następnie należy wpisać polecenie connection. Pojawi się informacja, że aktualnie znajdujemy się w opcji fsmo maintenance, gdzie należy wpisać polecenie connections. W tym kroku podłączamy się do kontrolera domeny, na który zostaną przeniesione role fsmo. Następnie należy wpisać connect to server dc2016.elitepc.local. Zostanie wyświetlona informacja o nawiązaniu połączenia z serwerem dc2016. W kolejnym kroku należy wpisać quit, co spowoduje automatyczny powrót do kroku fsmo maintenance, gdzie następnie zostanie przeprowadzona migracja ról fsmo. Kolejno należy wpisać:

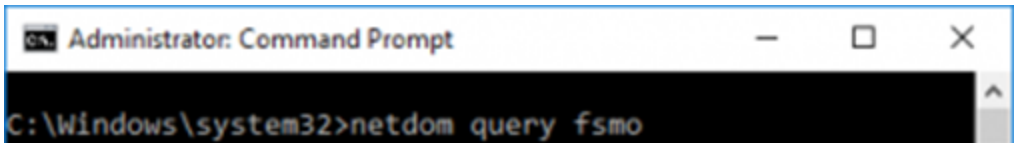
- transfer pdc,
- transfer naming master,
- transfer schema master,
- transfer rid master,
- transfer infrastructure master.

Na koniec należy wyjść z fsmo maintenance za pomocą polecenia quit i dalej z narzędzia ntdsutil również za pomocą polecenia quit.

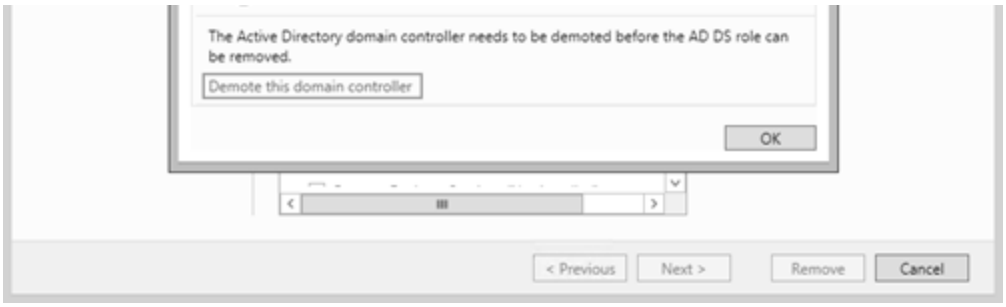


36. Deinstalacja starego kontrolera domeny

Gdy role FSMO zostały przeniesione na nowy kontroler domeny, można ponownie sprawdzić, na którym kontrolerze domeny aktualnie znajdują się role FSMO.



Po poprawnym przeniesieniu ról FSMO można zdepromować stary kontroler domeny. W tym celu, z poziomu starego kontrolera domeny dc.farbenia.pl, z Server Managera należy wybrać opcję Remove Roles and Features, następnie w kroku Server Roles odznaczyć Active Directory Domain Services i DNS Server. Pojawi się informacja, że jest to kontroler domeny i przed usunięciem wybranych elementów należy zdepromować kontroler domeny za pomocą przycisku Demote this domain controller.

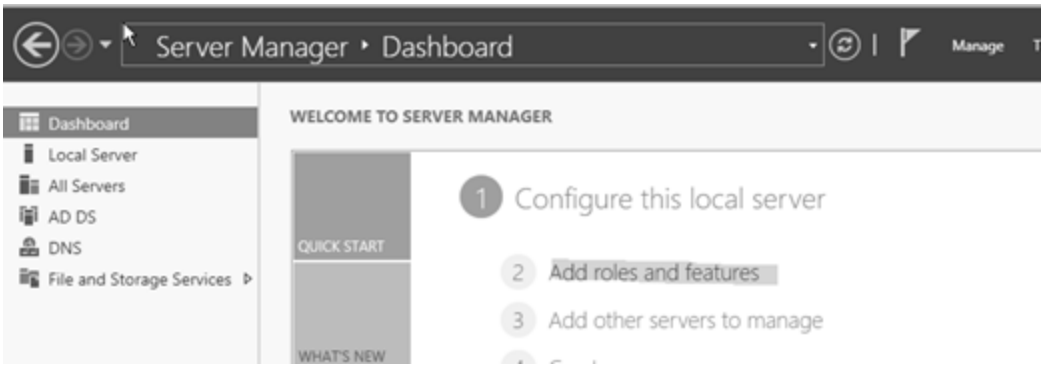


Gdy aktualny kontroler domeny zostanie zdepromowany, serwer można usunąć z domeny, jedynym i aktualnym kontrolerem domeny, który przechowuje wszystkie role FSMO, jest serwer dc2016.

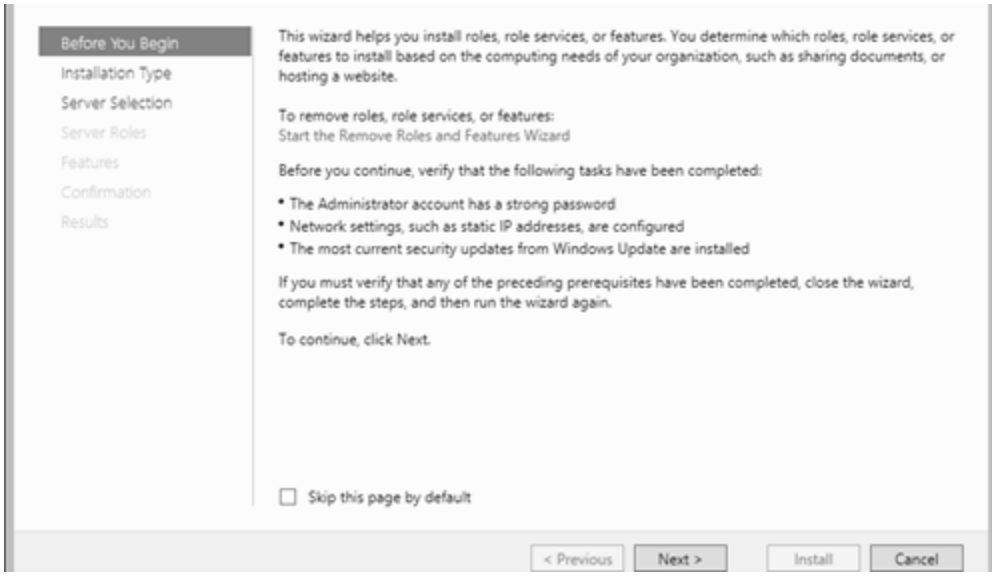
37. Przywracanie usługi Active Directory po katastrofalnej awarii

Należy zainstalować Windows Server Backup. Windows 2016 umożliwia utworzenie i przywrócenie kopii zapasowej.

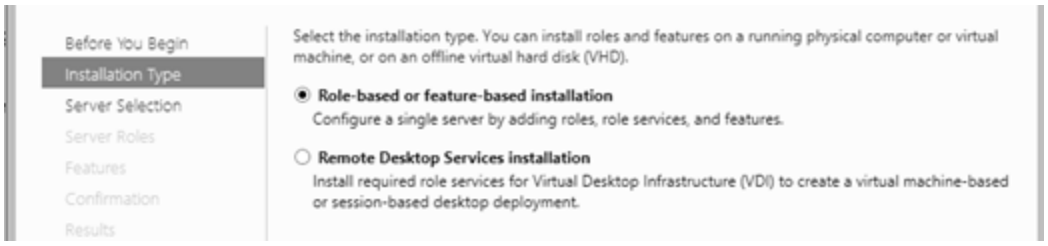
Aby rozpocząć instalację, należy przejść do Server Manager i kliknąć Add roles and features.



Następnie należy kliknąć Next.

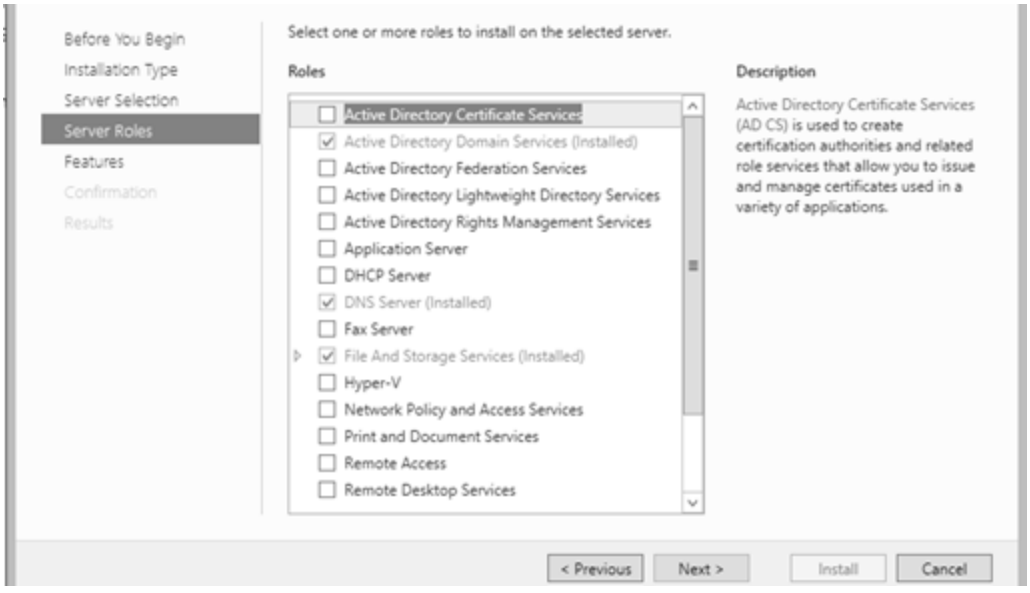


Na kolejnej karcie ponownie należy kliknąć Next.

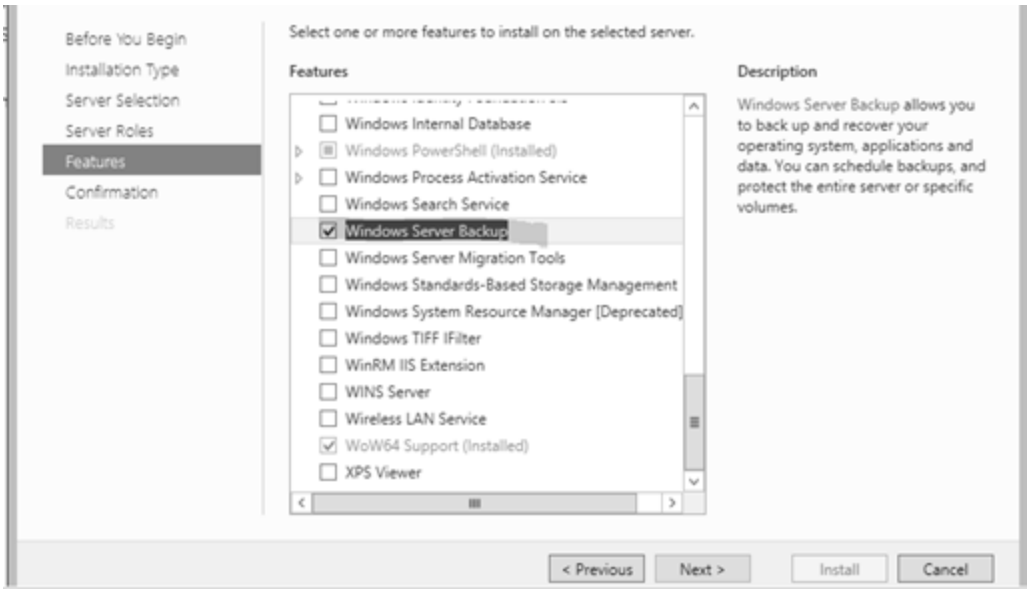


Raz jeszcze należy kliknąć Next.

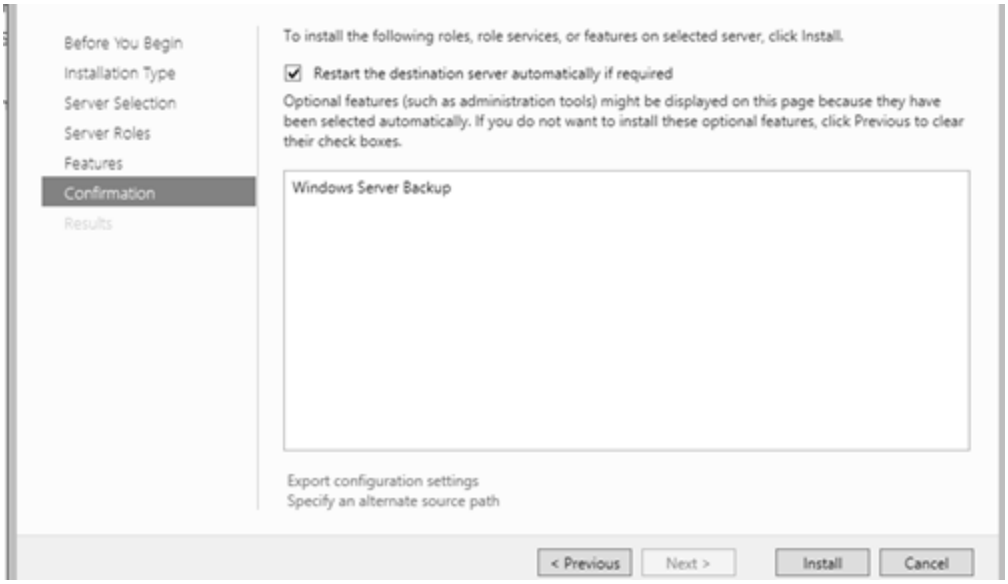
Ponownie należy kliknąć Next.



Dalej należy wybrać Windows Server Backup i kliknąć Next.



Znów należy kliknąć Next.



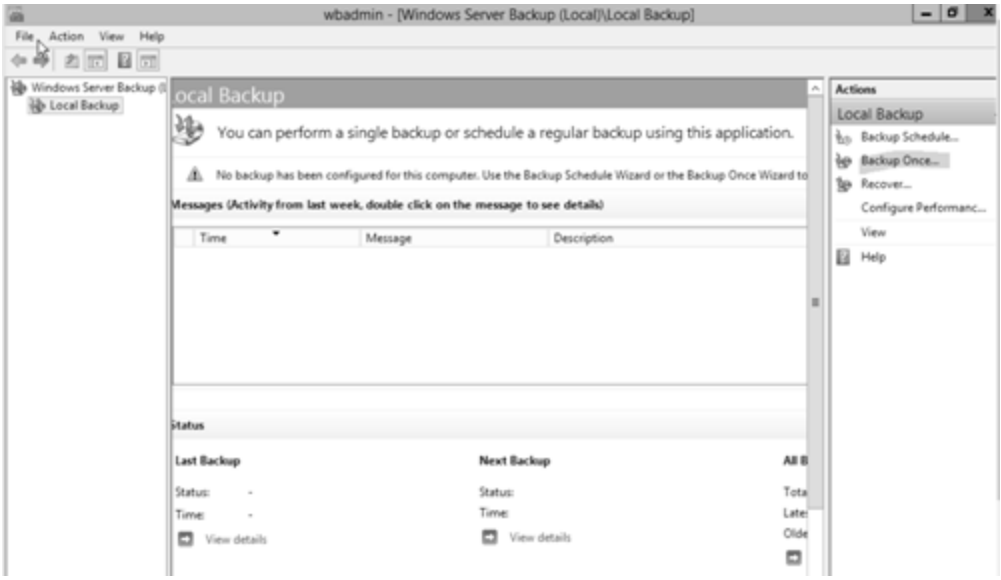
Po zakończeniu instalacji można zamknąć instalator.

38. Wykonywanie kopii zapasowej systemu

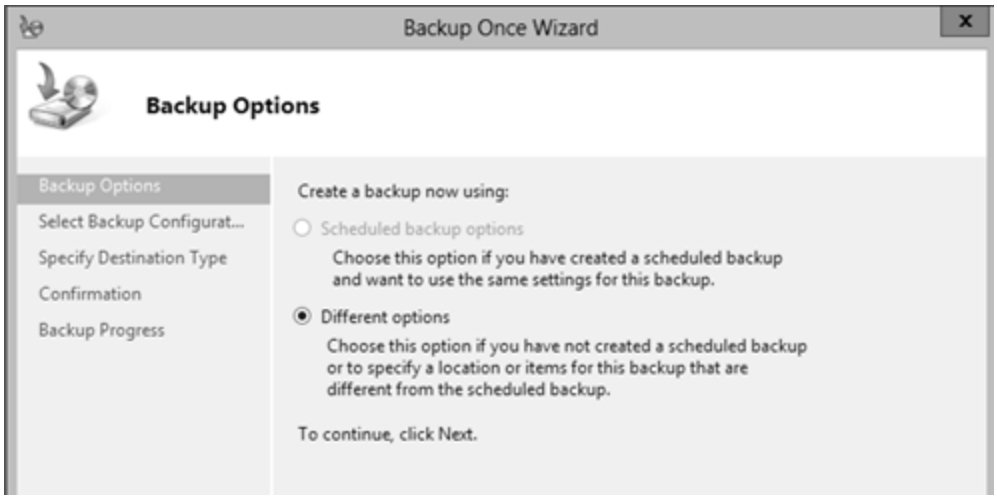
Można to zaplanować. Zademonstruję wykonanie jednej kopii zapasowej.

Należy otworzyć Server Manager, kliknąć na Tools i przejść do Windows Server Backup.

Następnie należy przejść do Local Backup i zrobić kopię zapasową (system backup).

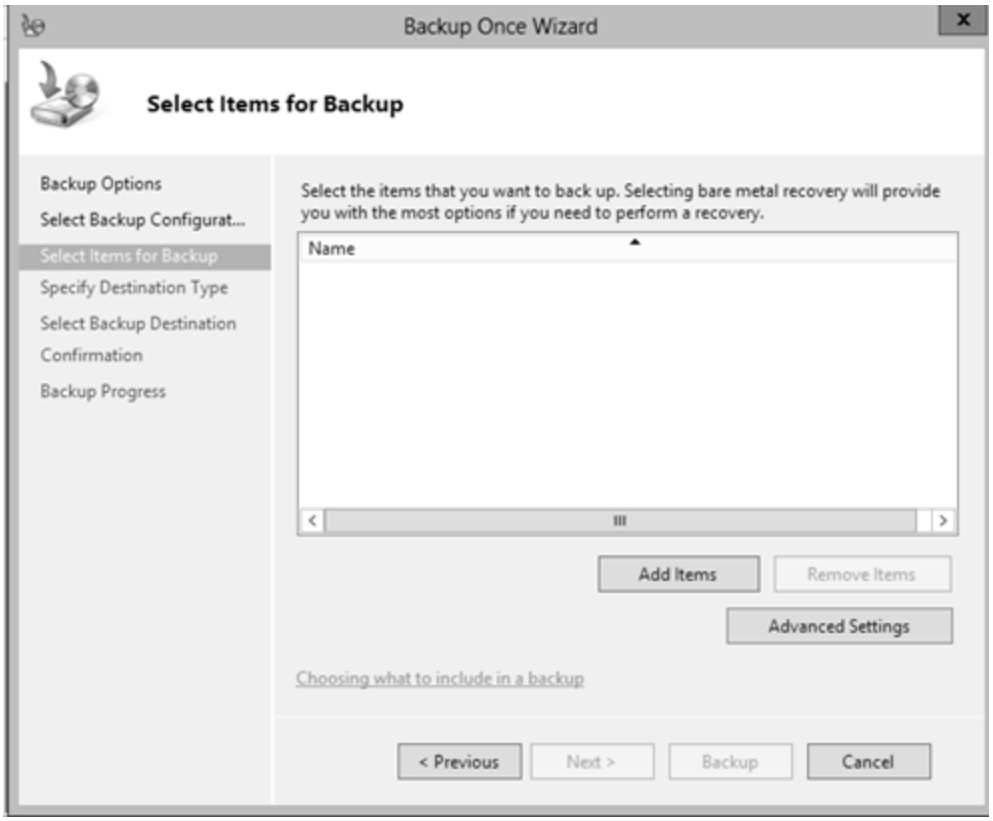


W kolejnym oknie ponownie należy kliknąć Next.

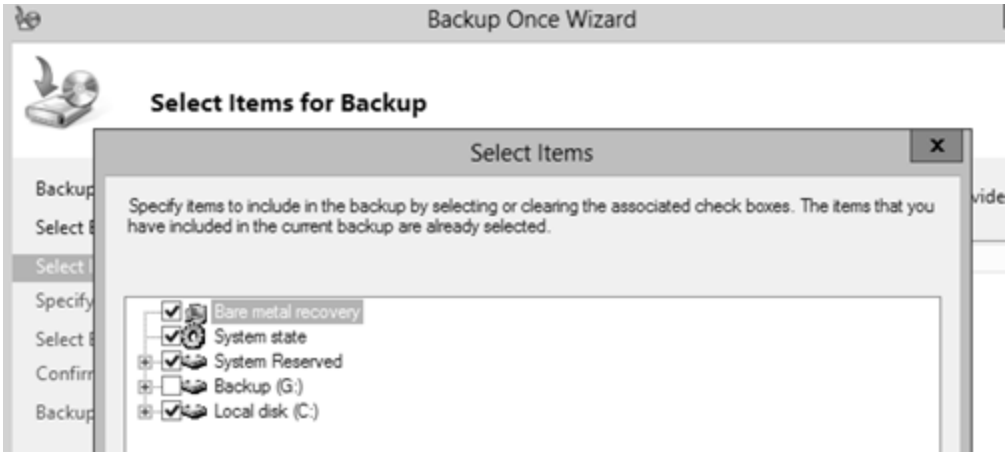


Dalej należy wybrać Custom i kliknąć Next.

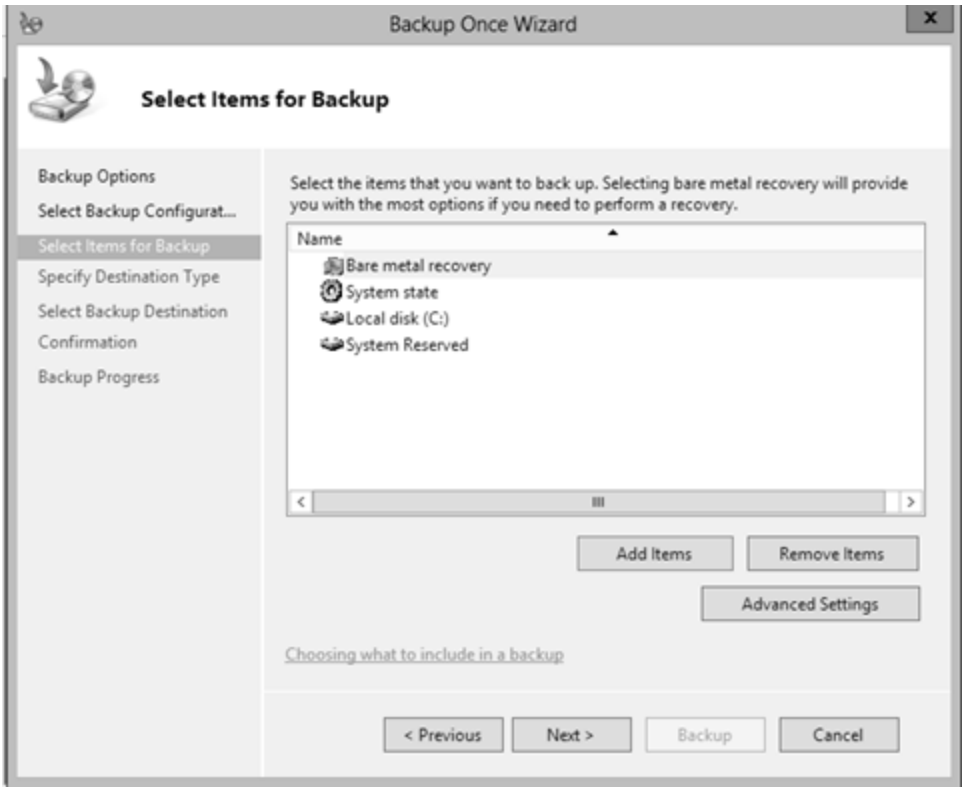
Należy kliknąć Add Items.



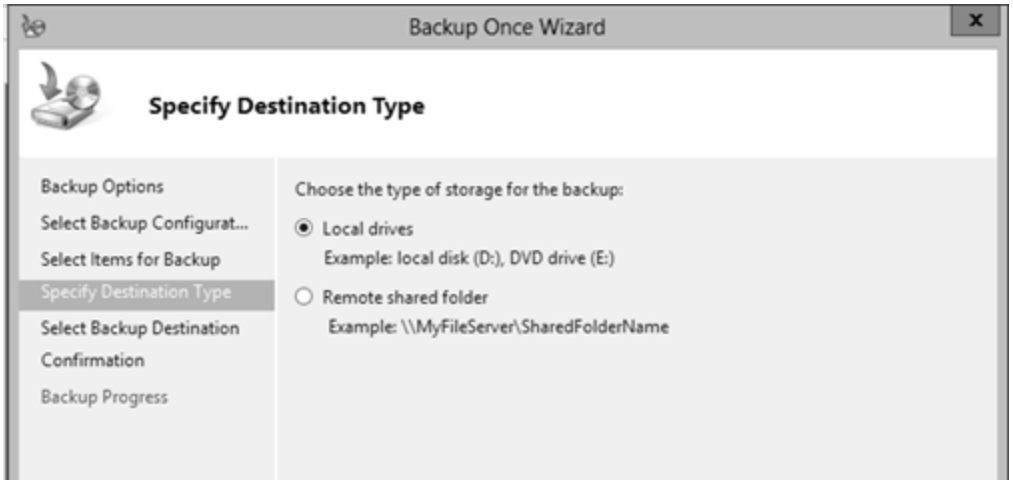
Teraz należy wybrać Backup Items i kliknąć OK.



Można przejść dalej, klikając Next.

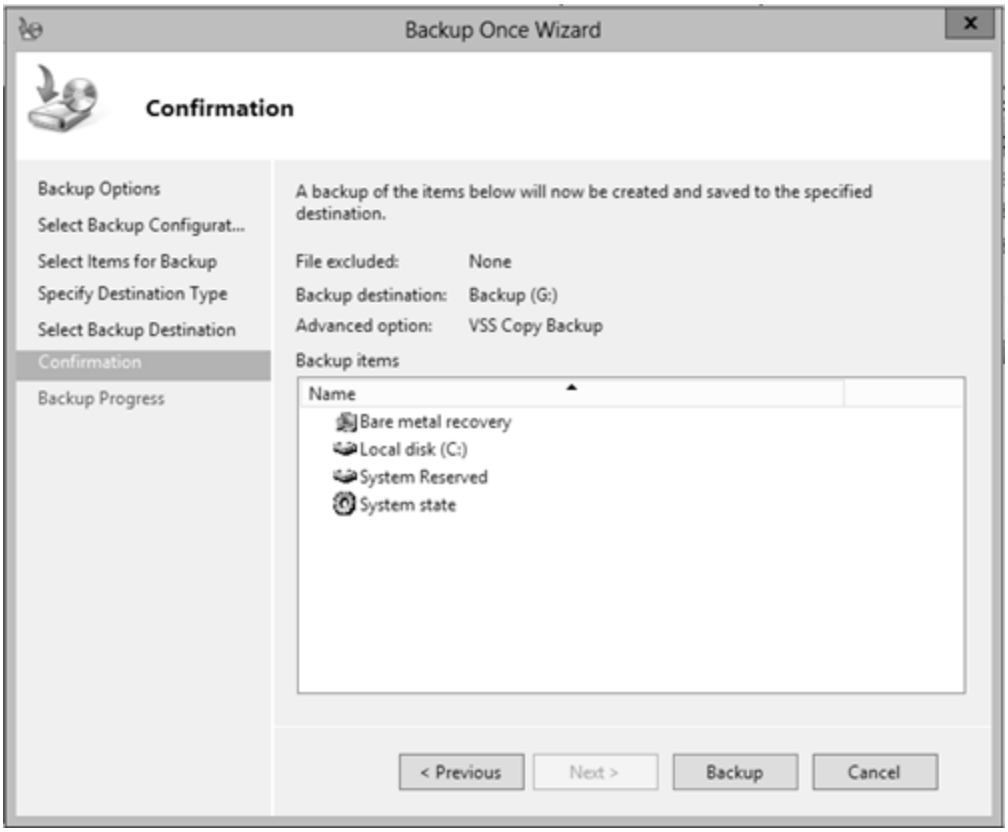


Następnie należy wybrać lokalizację, w której chcemy przechować kopię zapasową.

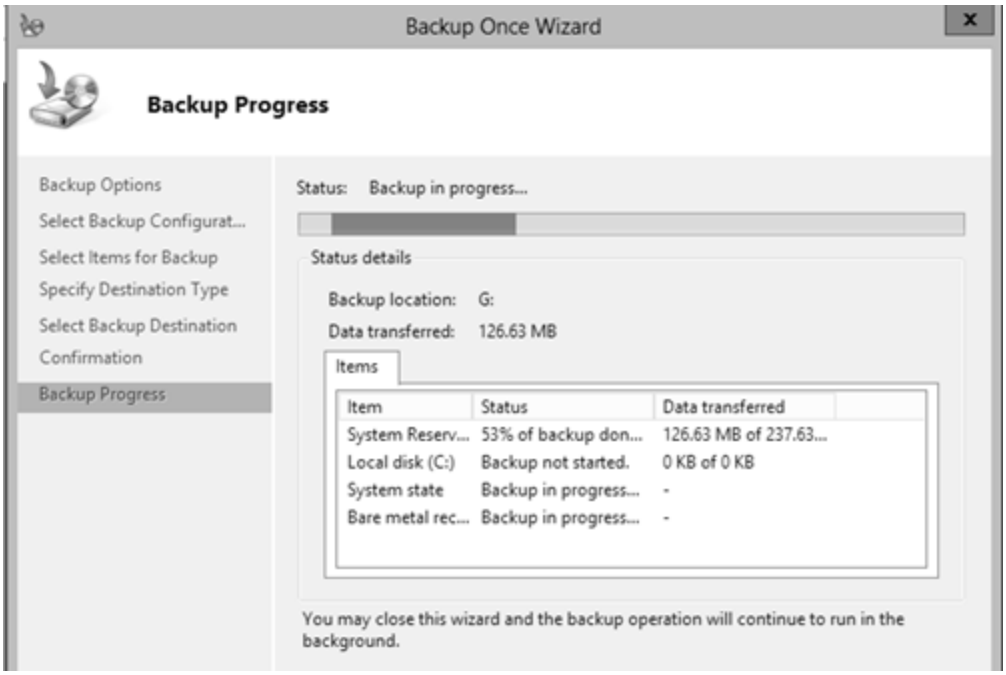


Zanim będzie można pójść dalej, należy sprecyzować Lokalizację sieciową (można również sprecyzować lokalny dysk) i następnie kliknąć Next.

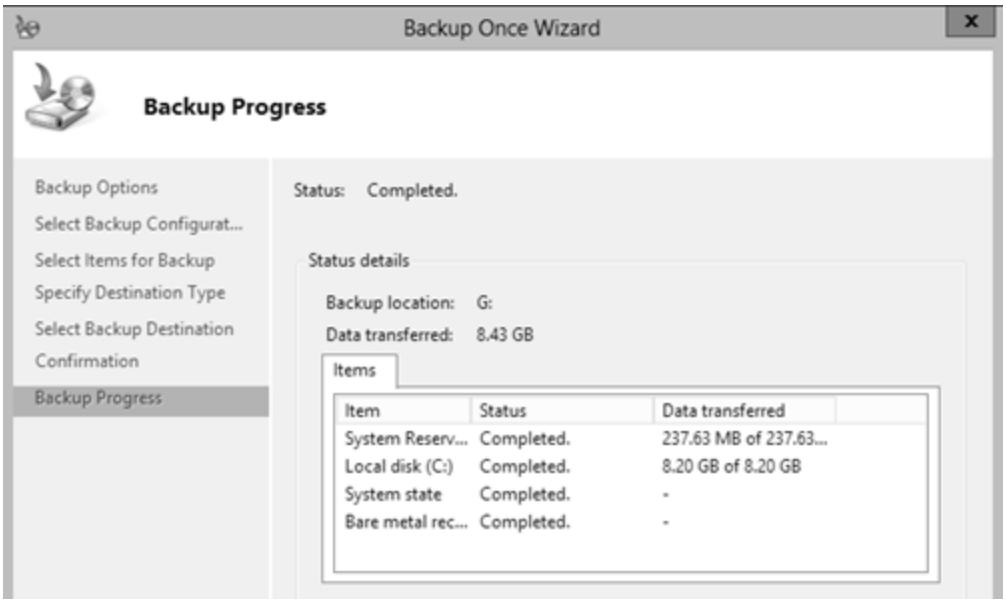
Należy potwierdzić wybór kopii zapasowej i kliknąć Backup.

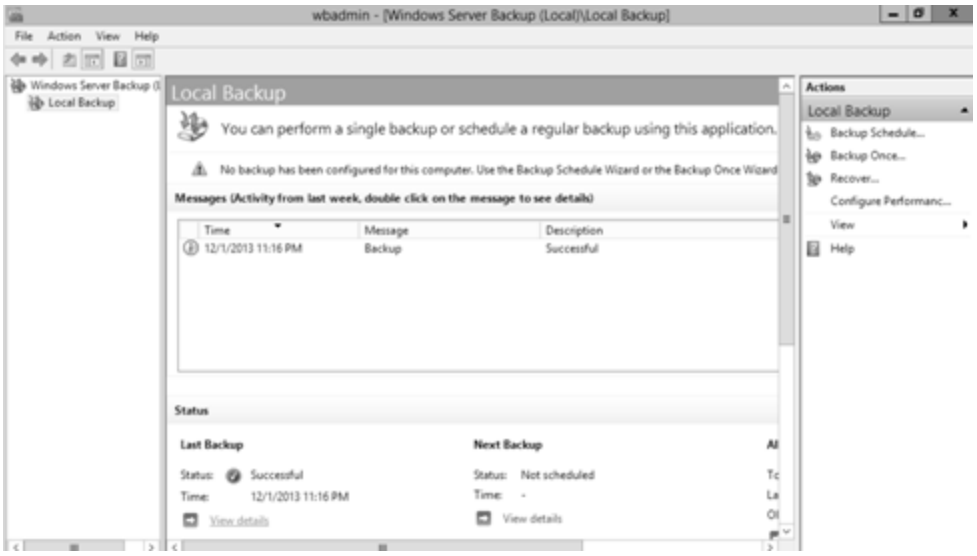


Teraz można już monitorować postęp tworzenia kopii zapasowej.

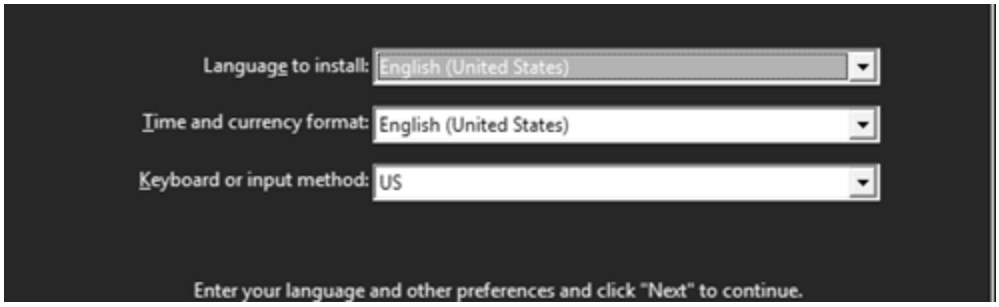


Gdy kopia zapasowa będzie gotowa, należy kliknąć Finish.

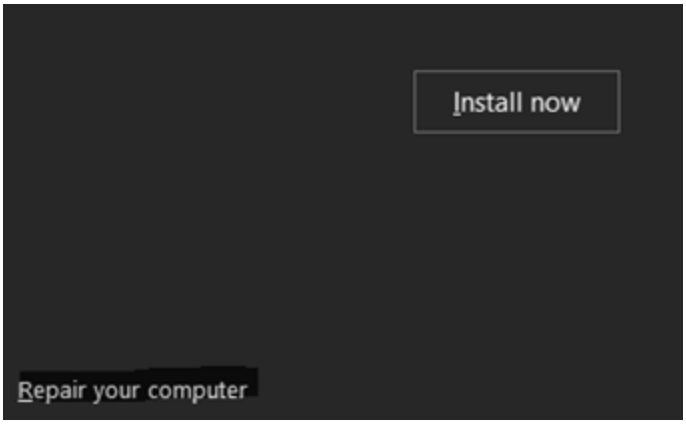




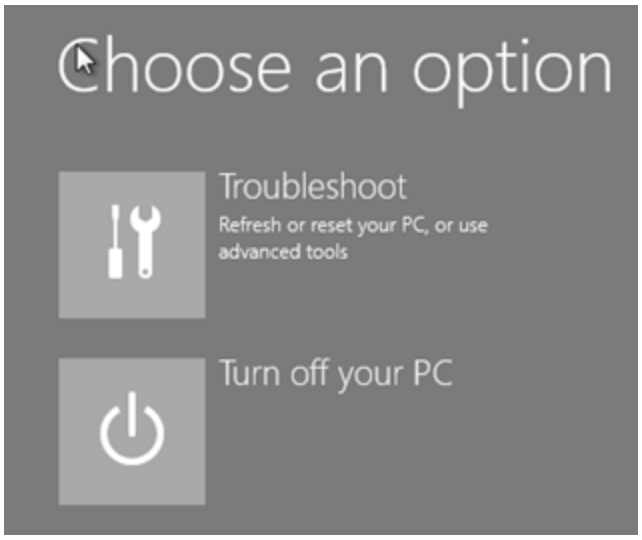
Można teraz rozpocząć instalacjęOS na serwerze.



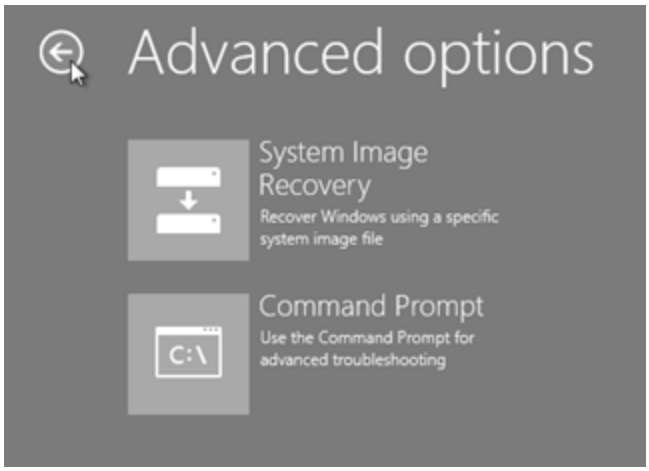
W tym celu należy kliknąć Repair your computer.



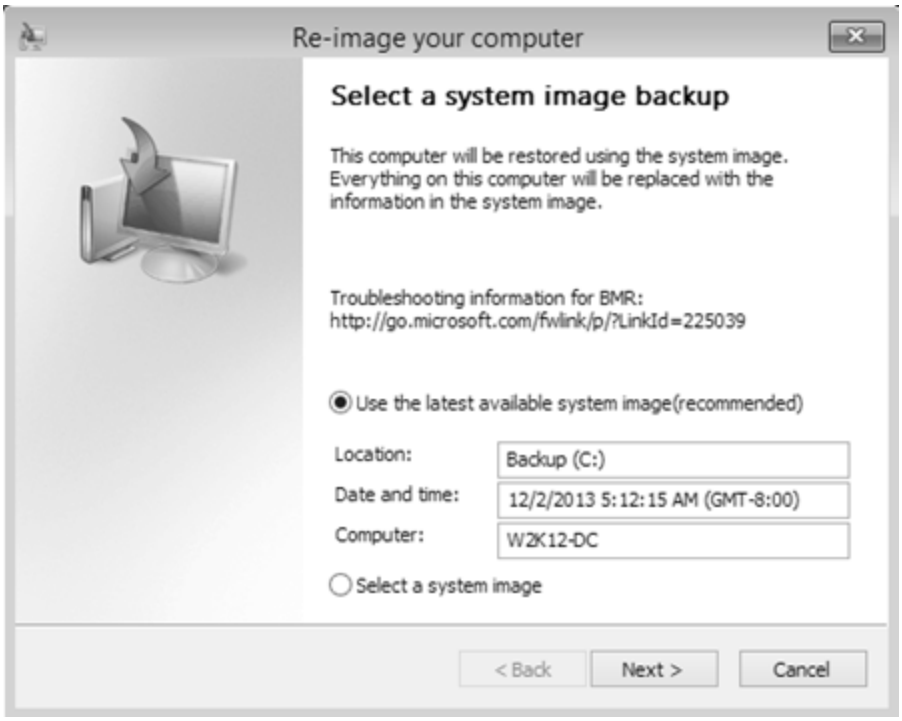
Następnie należy wybrać opcję Troubleshoot.



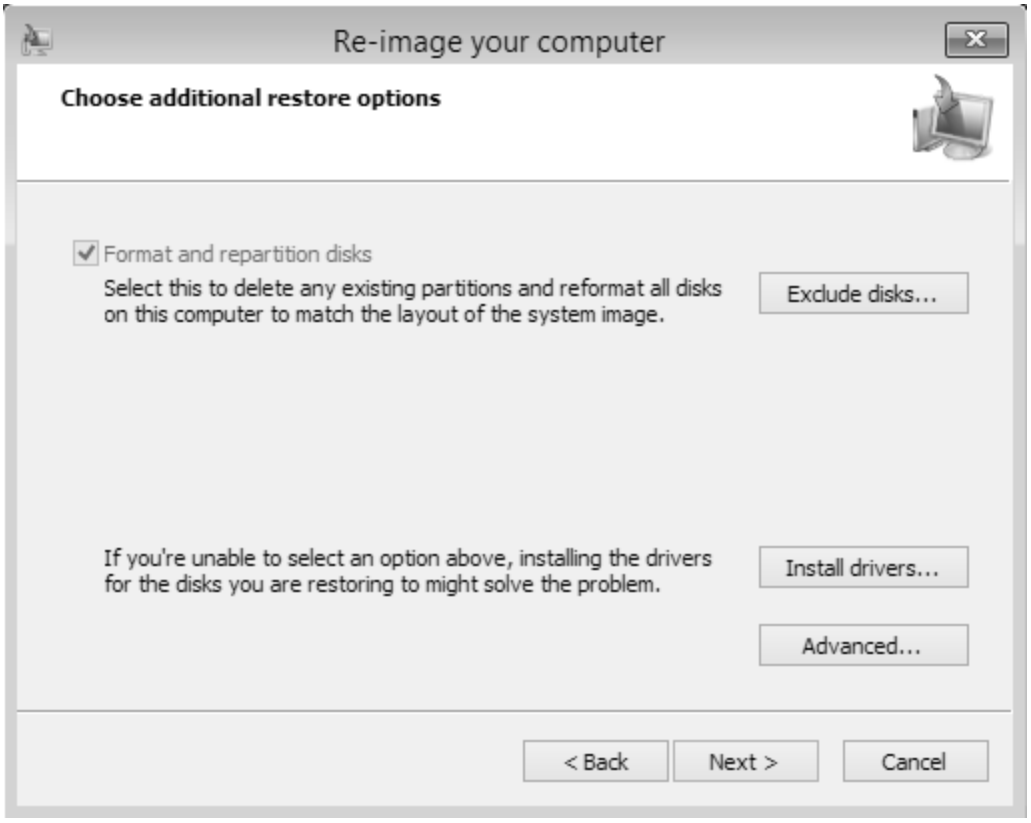
W kolejnym kroku należy wybrać System Image Recovery.



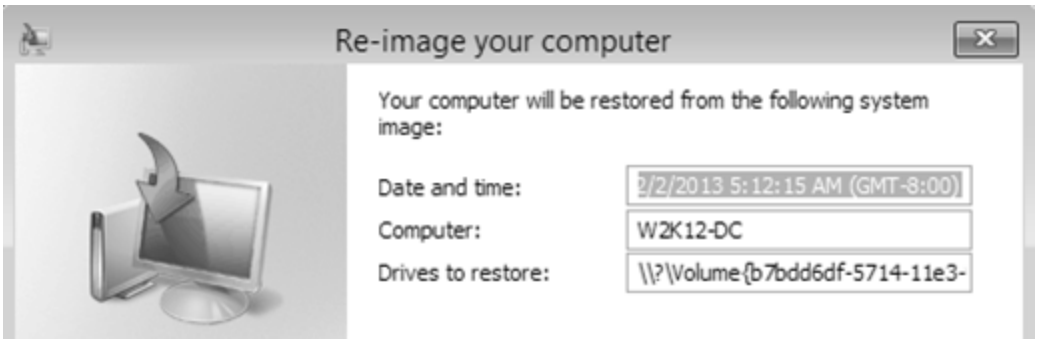
Obraz kopii zapasowej zostanie automatycznie wykryty z dysku lokalnego. Można wówczas kliknąć Next.



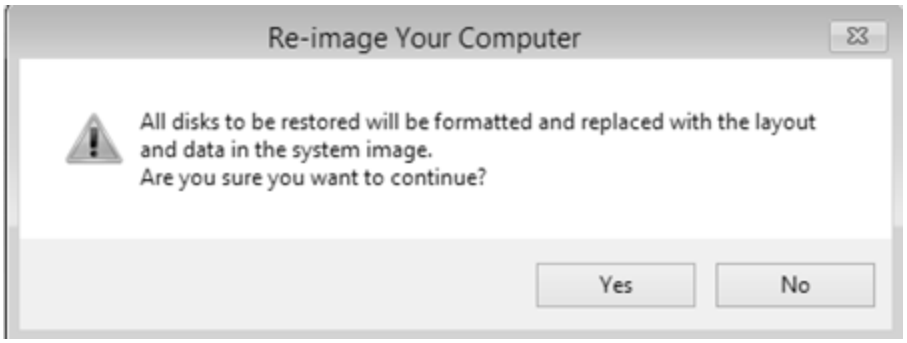
Ponownie należy kliknąć Next.



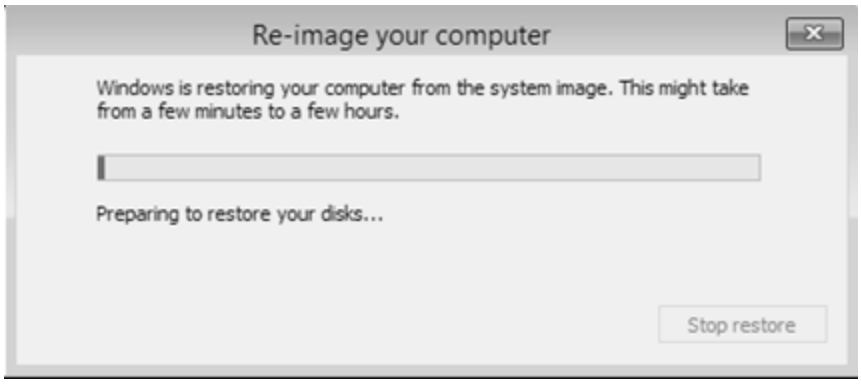
Aby zakończyć, należy kliknąć Finish.



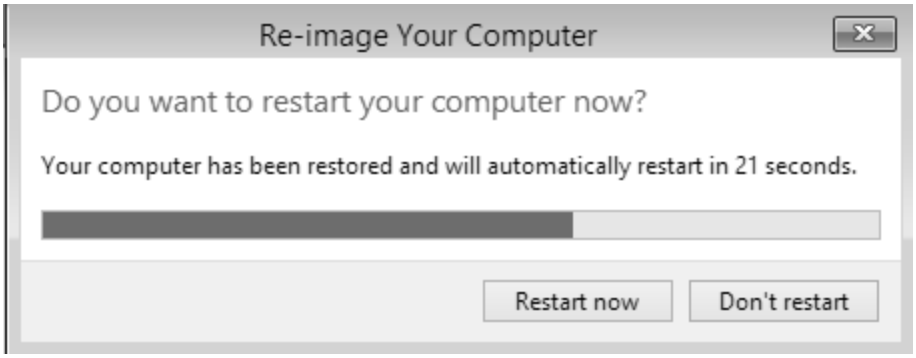
Aby przejść dalej, należy nacisnąć Yes.



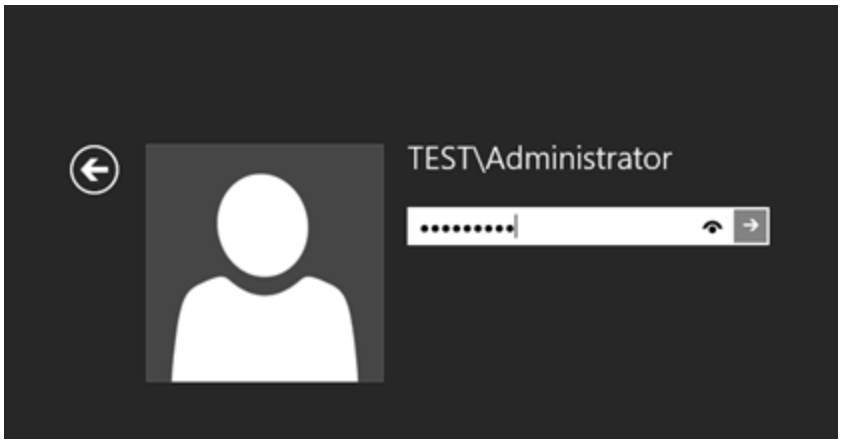
Proces przywracania zostanie rozpoczęty.



W kolejnym oknie należy kliknąć Restart Now.



Gdy serwer zacznie działać, będzie to nasz stary DC.

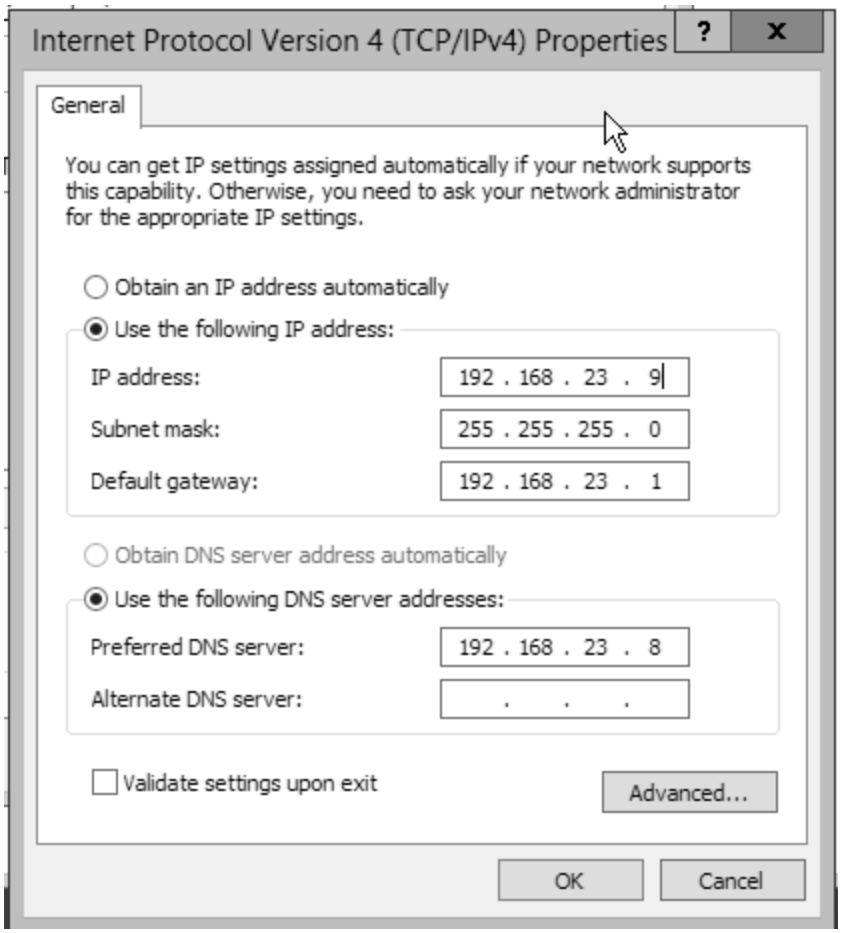


Można teraz sprawdzić właściwości systemu, aby to potwierdzić.

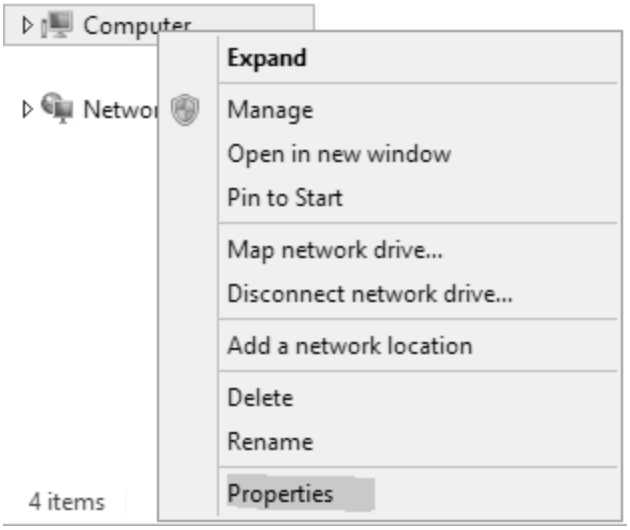
39. Dodatkowy kontroler domeny

W tym rozdziale zawarto informacje o dodaniu dodatkowego kontrolera domeny, który zadziała, gdyby podstawowy DC przestał działać. Należy najpierw skonfigurować statyczny adres IP, podstawowy DNS będzie istniejącym serwerem DNS, a drugorzędny będzie adresem IP samego serwera, więc będzie także działać jako pomocniczy serwer DNS. W przypadku awarii pierwszego DC, ten serwer zapewni usługi AD i DNS do sieci.

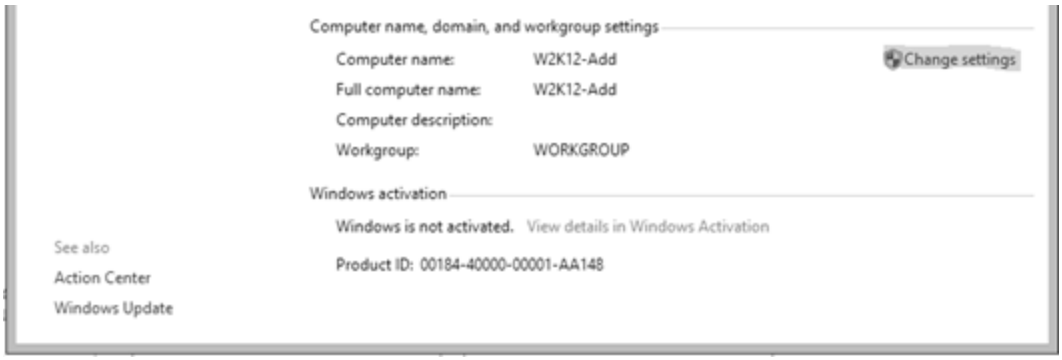
Należy zacząć od skonfigurowania Statycznego IP.



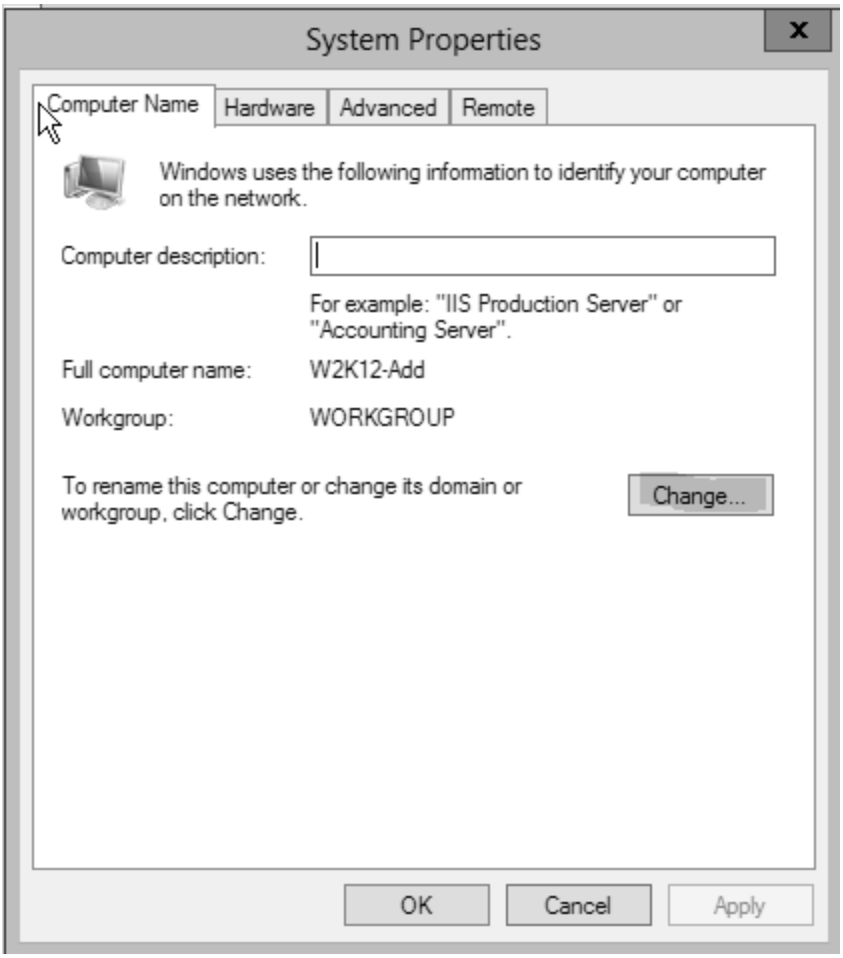
Aby dodać serwer do domeny, trzeba nacisnąć prawym przyciskiem myszy na Computer i przejść do properties (lub można przejść do system z Control Panel).



Następnie należy kliknąć Change Settings.

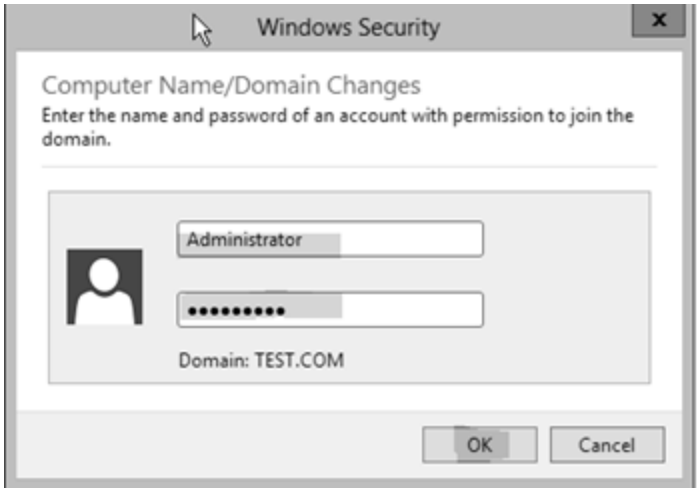


Dalej należy kliknąć Change na System Properties.

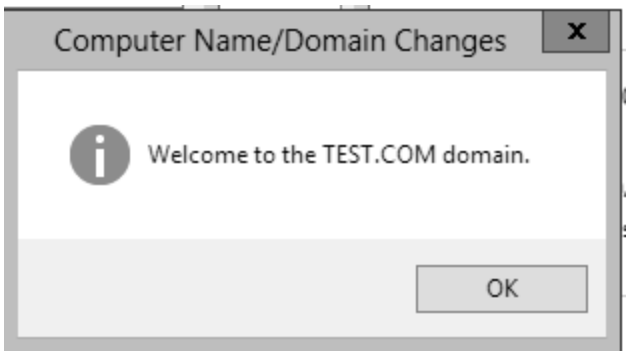


W kolejnym kroku trzeba wybrać Domain, wpisać nazwę domeny i kliknąć OK.

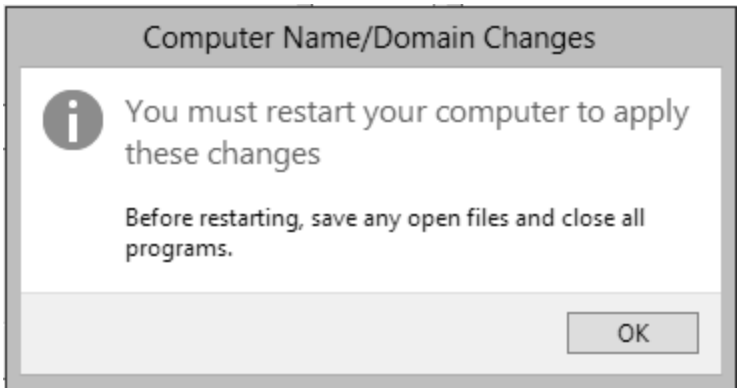
W kolejnym oknie należy wpisać dane Admina i kliknąć OK.



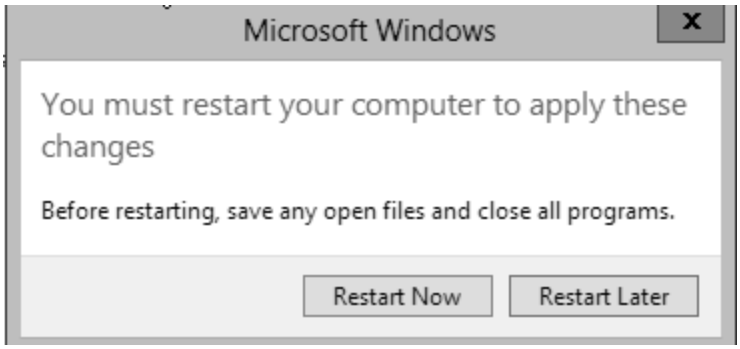
Ponownie należy kliknąć Ok.



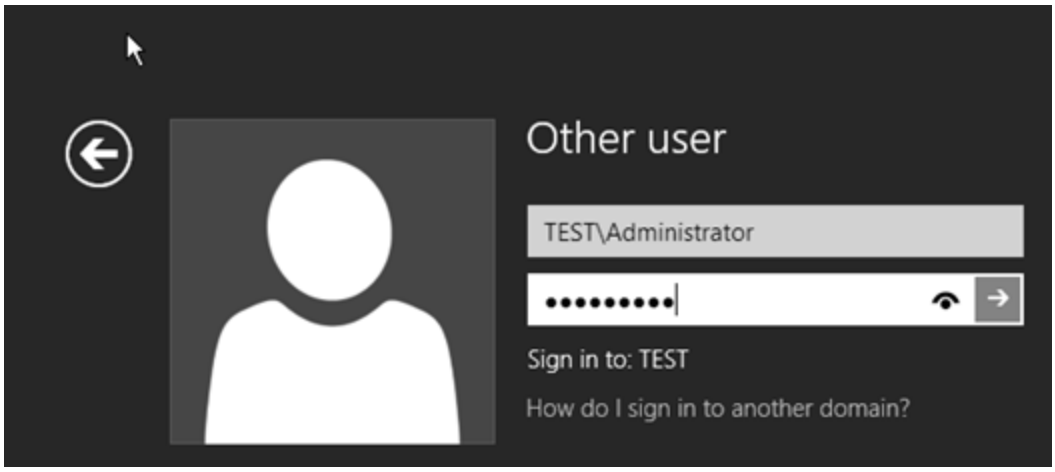
Jeszcze raz należy kliknąć OK.



A następnie można zamknąć System Properties i kliknąć Restart Now.

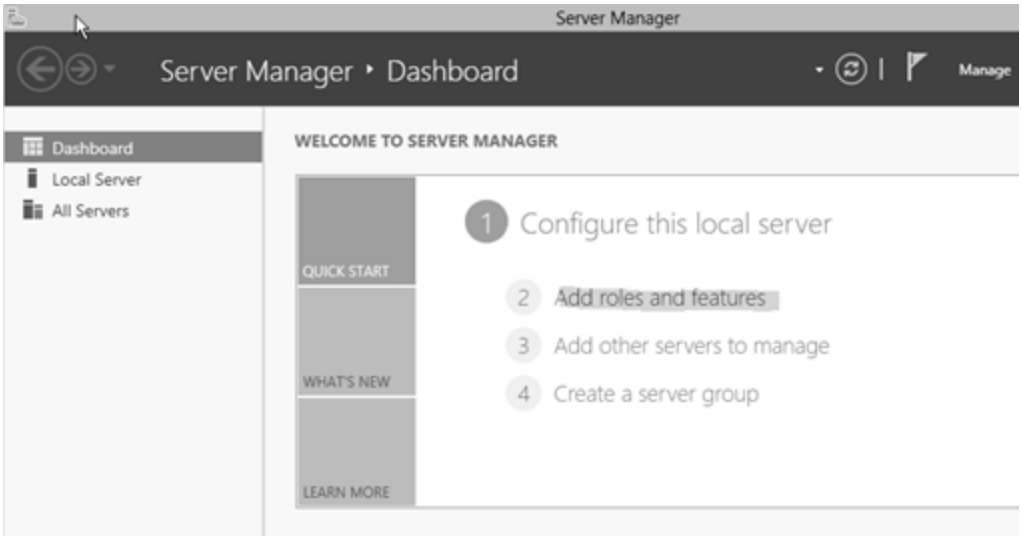


Gdy system uruchomi się ponownie, należy zalogować się danymi Domeny.

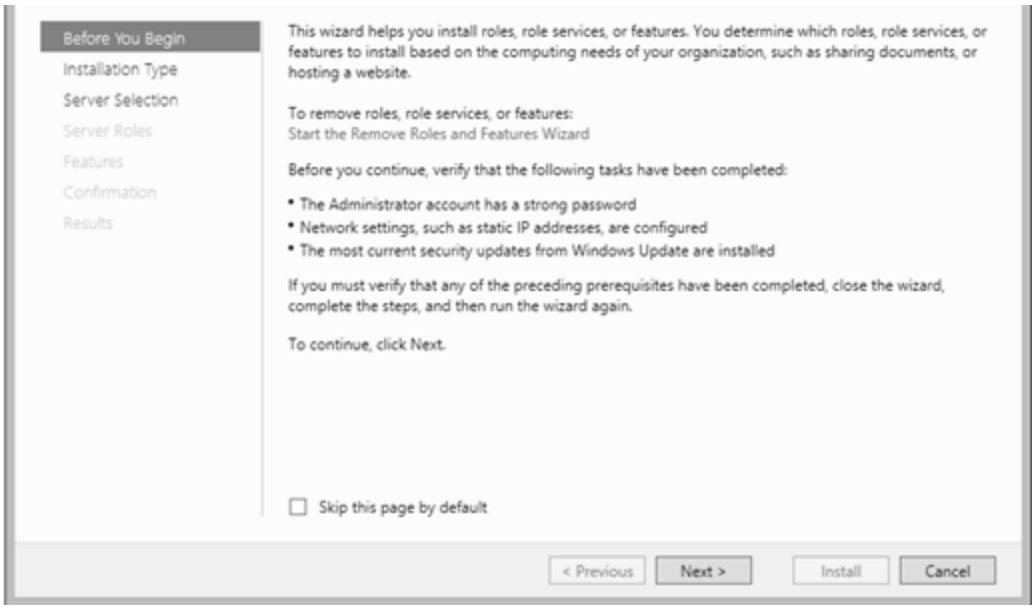


40. Instalacja AD Role na Serwerze

Należy otworzyć Server Manager i kliknąć Add Roles and Features.

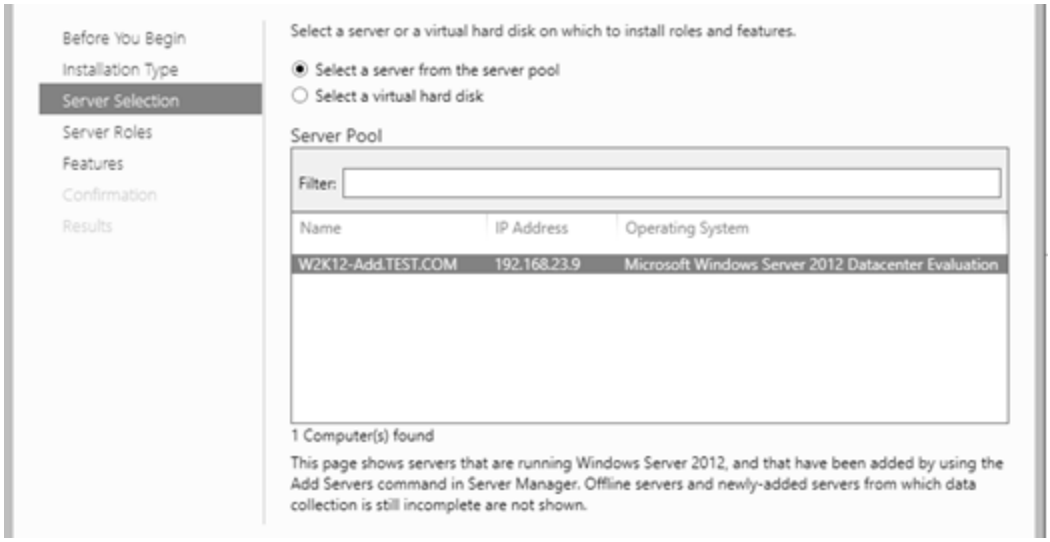


Następnie należy kliknąć Next na ekranie Before you Begin.

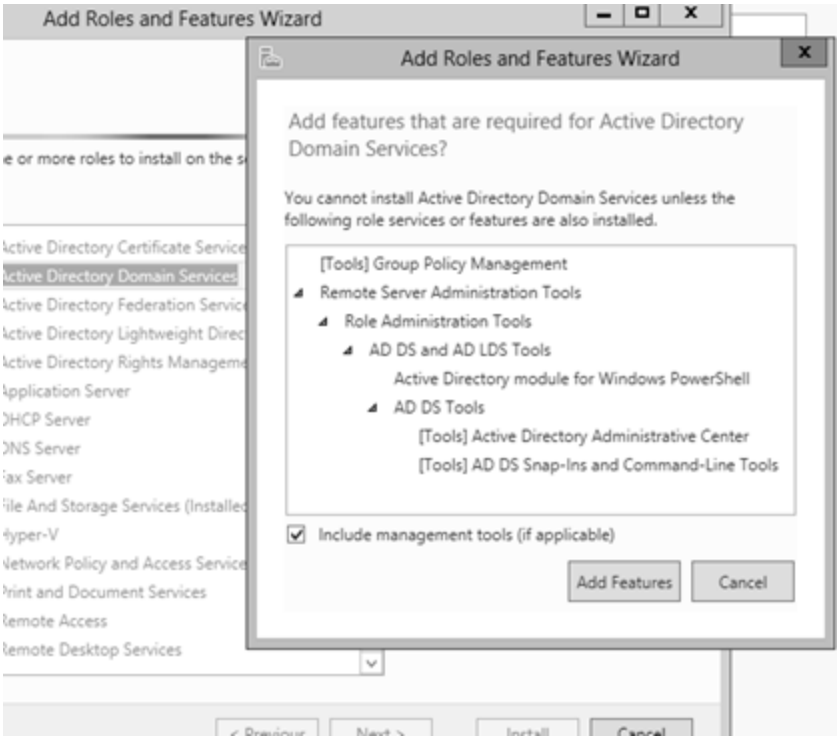


Ponownie należy kliknąć Next.

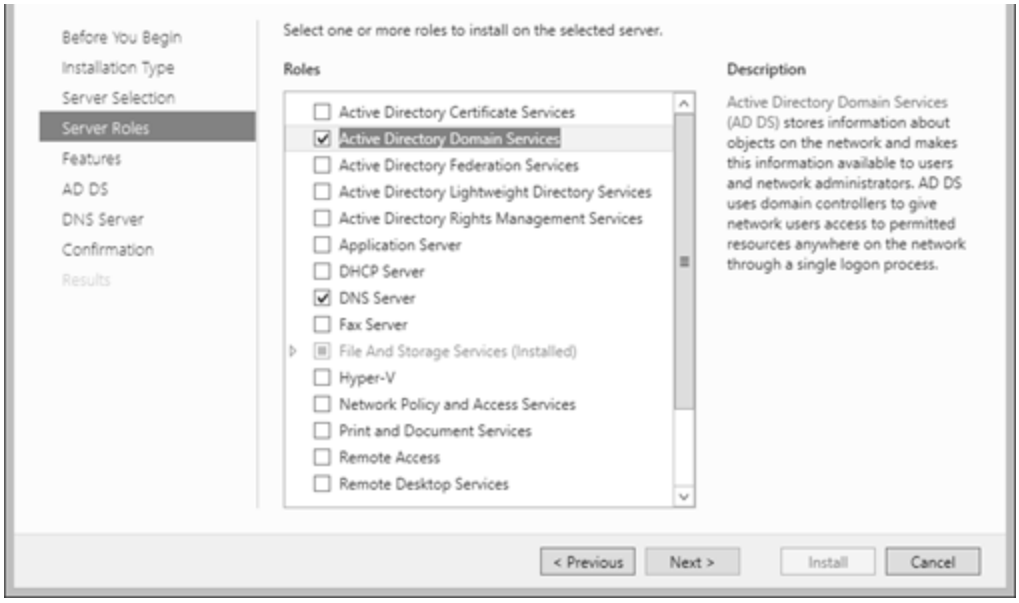
Aby przejść dalej, należy wybrać Serwer i kliknąć Next.



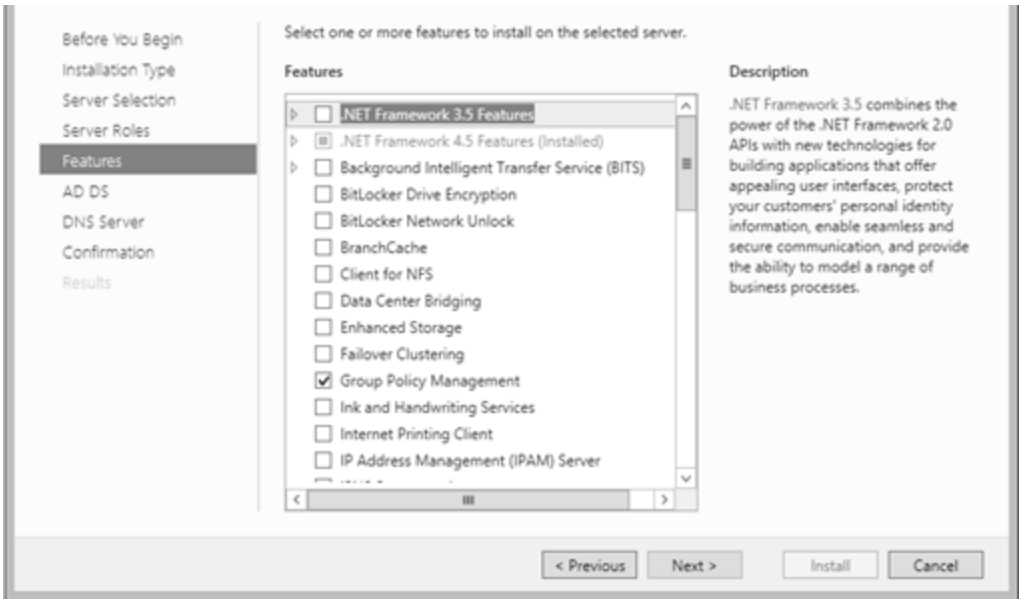
Następnie należy wybrać Active Directory Domain Services oraz kliknąć Add Features na wyskakującym oknie.



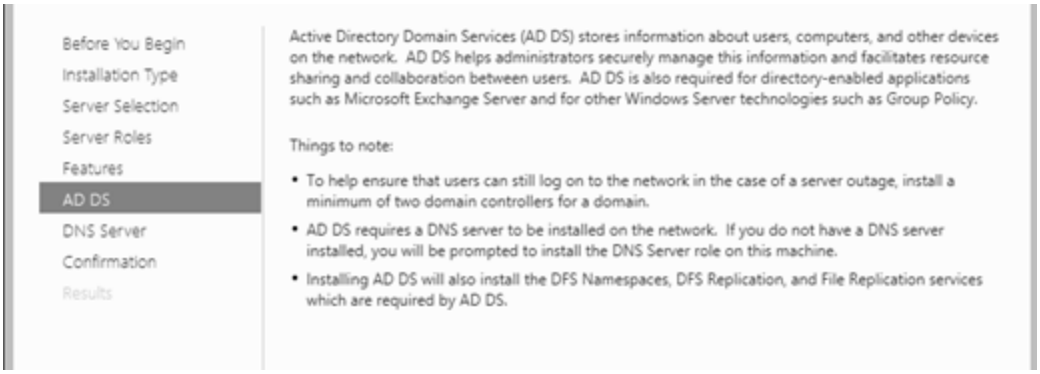
Ponownie należy kliknąć Next. Jeśli chcemy uczynić ten serwer również dodatkowym serwerem DNS, należy zaznaczyć to pole, w przeciwnym razie powinno pozostać niezaznaczone.



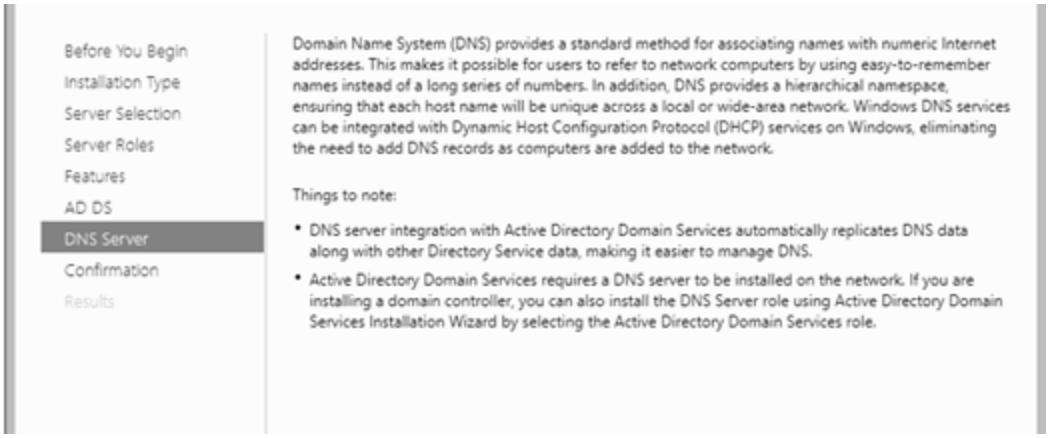
W kolejnym oknie należy kliknąć Next.



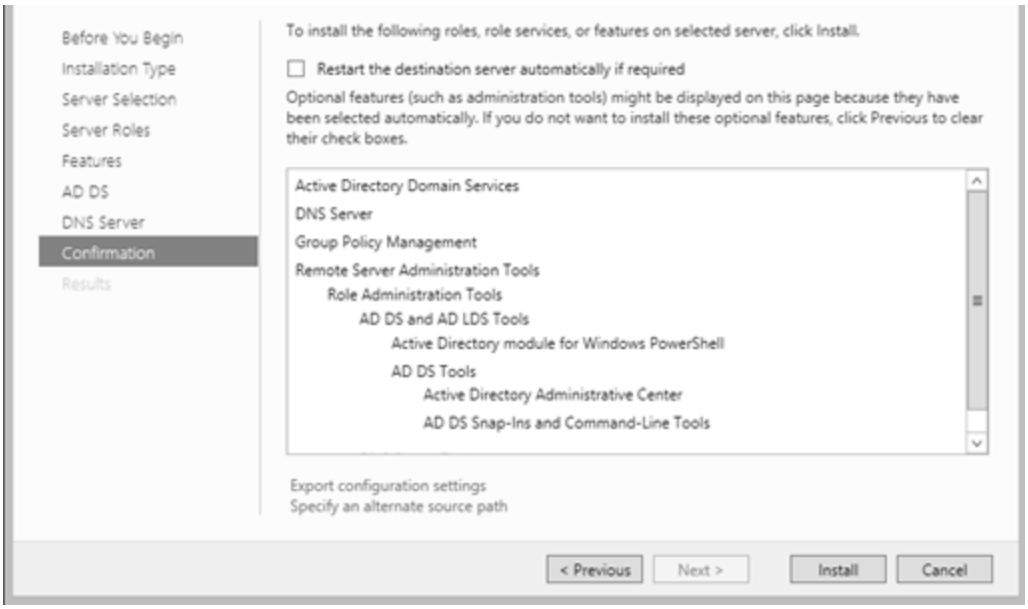
I ponownie trzeba kliknąć Next.



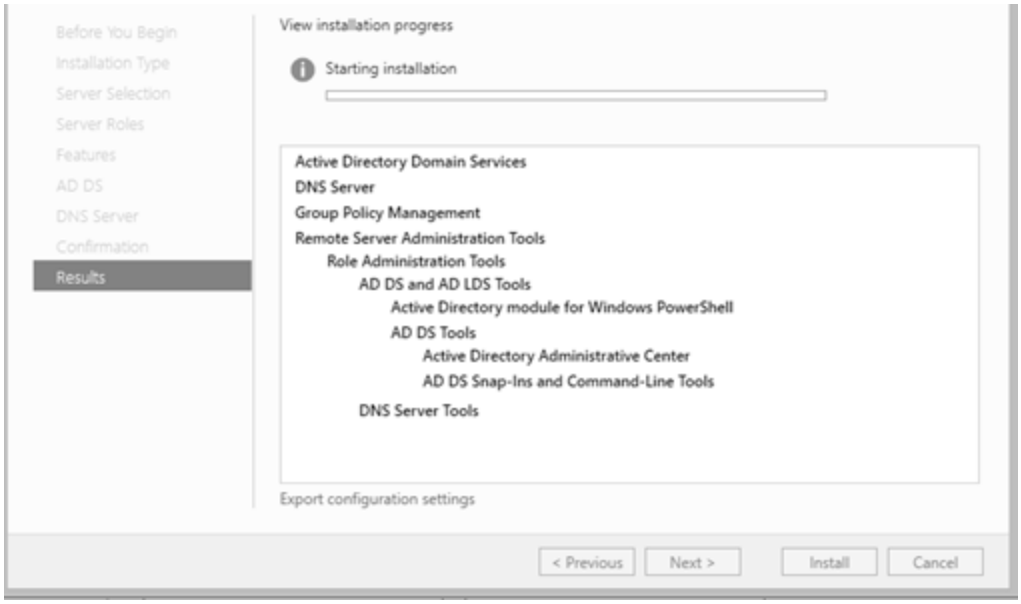
Znów należy kliknąć Next (ten ekran pojawi się tylko wówczas, gdy został wybrany DNS server role).



Teraz można już kliknąć Install.



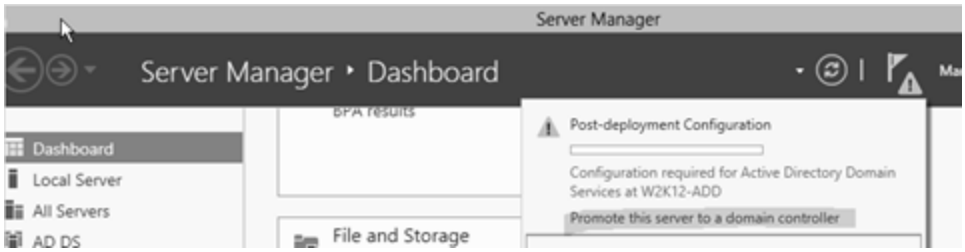
Rozpocznie się instalacja. Można teraz zamknąć to okno i obserwować postępy na pasku powiadomień.



Gdy instalacja się zakończy, należy kliknąć Close.

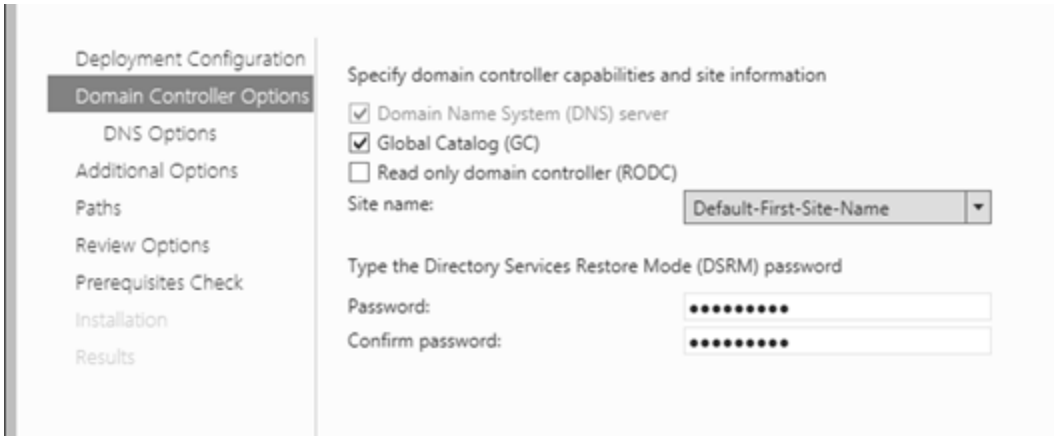
41. Awansowanie serwera na kontroler domeny

Aby awansować serwer na kontroler domeny, należy przejść do paska powiadomień, kliknąć na wykrzynk, a następnie Promuj ten serwer do kontrolera domeny.

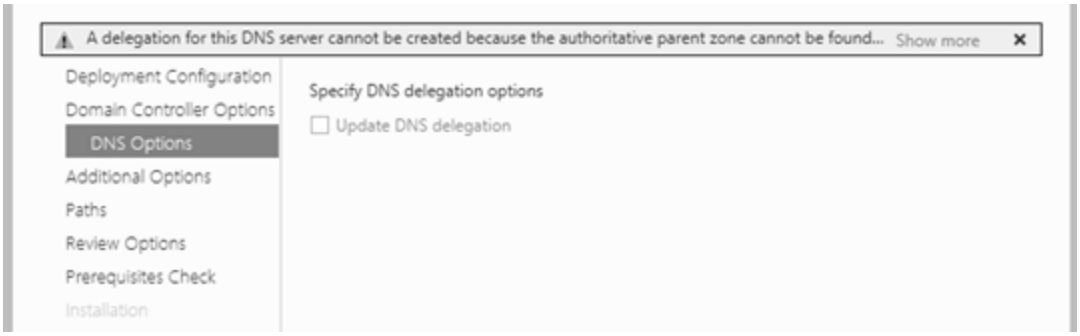


Teraz trzeba wybrać opcję Add a domain controller to an existing domain, wybrać domenę I wpisaćdane oraz kliknąć Next.

Teraz należy wybrać nazwę strony (default), dostarczyć hasło DSRM i kliknąć Next.

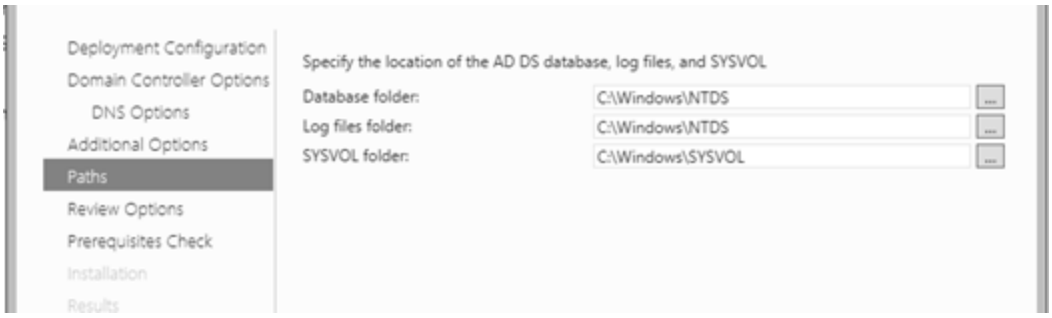


Ponownie należy kliknąć Next.

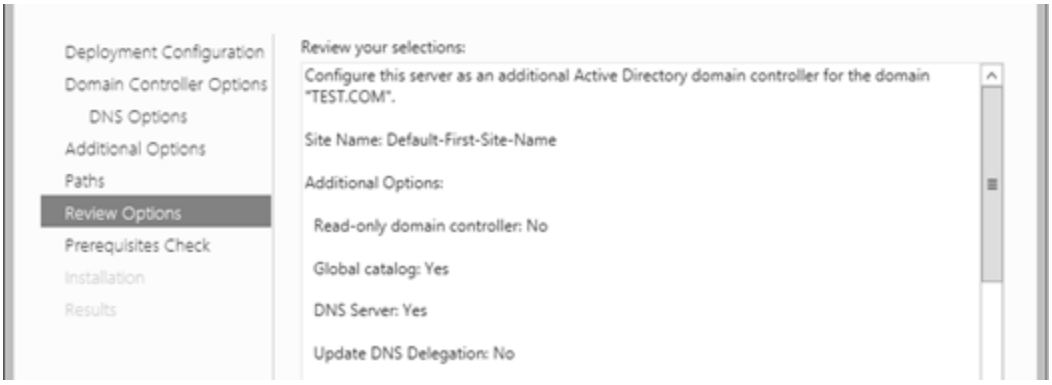


W kolejnym oknie należy wybrać DC, z którego będziemy replikować i kliknąć Next.

Teraz można już wybrać lokacje folderów database, log and SYSVOL , lub wybrać default i kliknąć Next.



Ponownie należy kliknąć Next.



Jeżeli wszystkie wymagania wstępne są zapewnione, należy kliknąć Install.

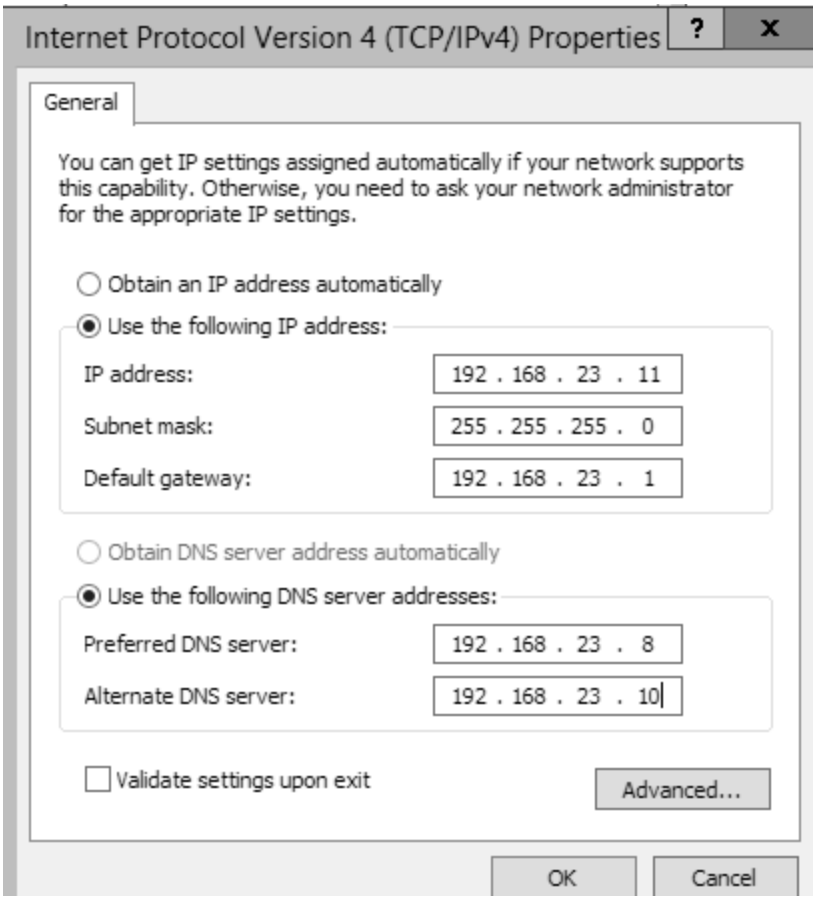
Po zakończeniu instalacji, należy kliknąć Close.

Serwer uruchomi się ponownie automatycznie po zakończeniu instalacji. Nasz serwer jest teraz skonfigurowany jako dodatkowy kontroler domeny.

42. Dodawanie domeny podrzędnej

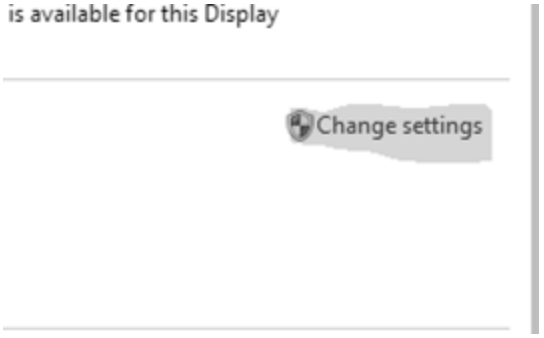
Aby utworzyć domenę poddomeny lub podrzędną, należy skonfigurować inny serwer, dodać go do domeny, zainstalować na nim rolę AD, a następnie promować ją jako DC, jako domenę podrzędną. Kroki są podane poniżej.

Krok 1. Konfiguracja statycznego IP

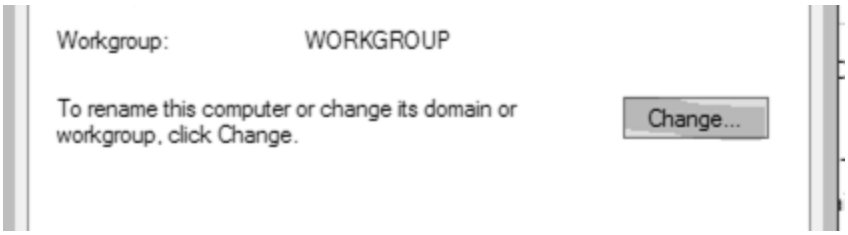


Krok 2. Dodanie serwera do domeny

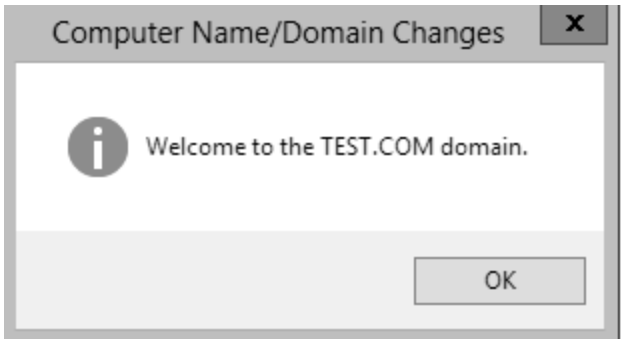
Należy przejść do Control Panel, otworzyć system i kliknąć na Change Settings.



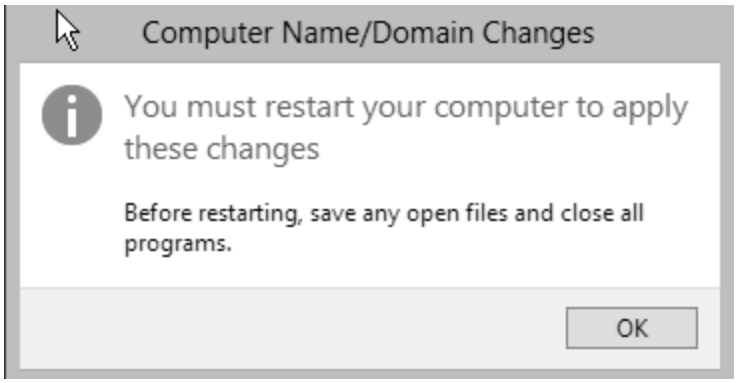
Teraz należy kliknąć Change system we właściwościach.



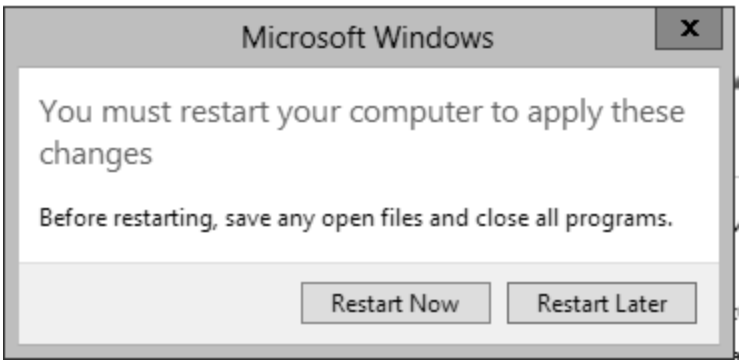
Po podaniu danych należy kliknąć OK.



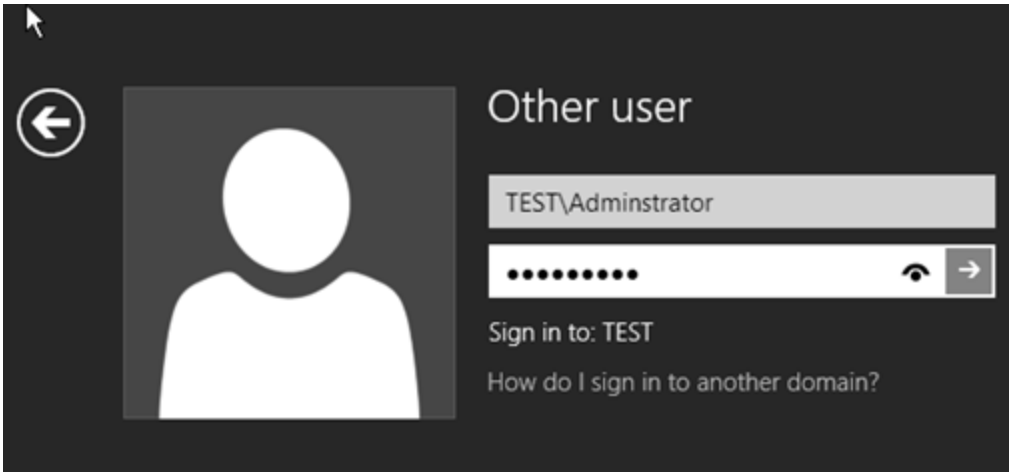
I ponownie należy kliknąć OK.



W następnym kroku należy zamknąć System Properties i kliknąć Restart Now.

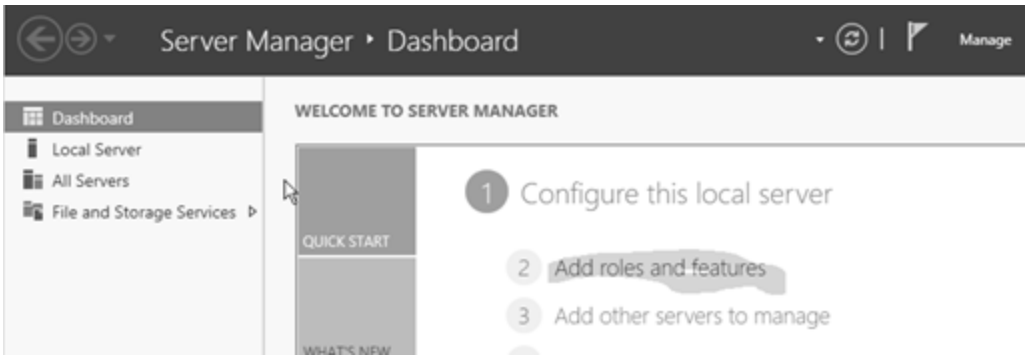


Gdy serwer się włączy, należy zalogować się do niego swoimi danymi.

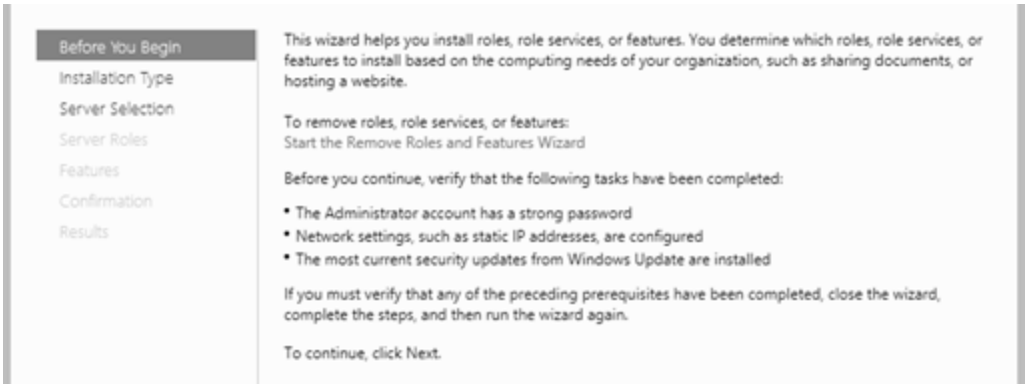


Krok 3. Instalacja roli AD

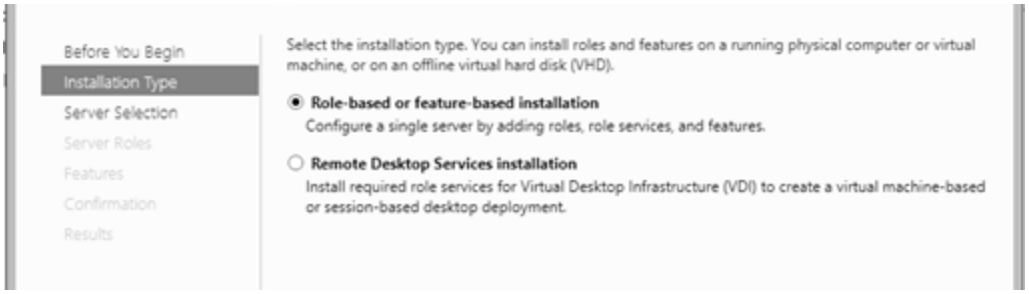
Teraz należy przejść do Server manager i kliknąć na Add roles and Features.



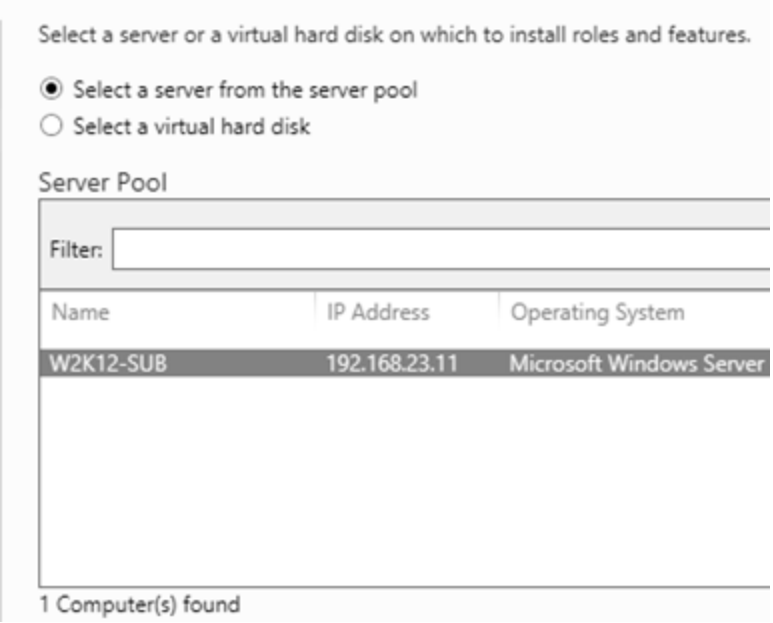
Następnie należy kliknąć Next.



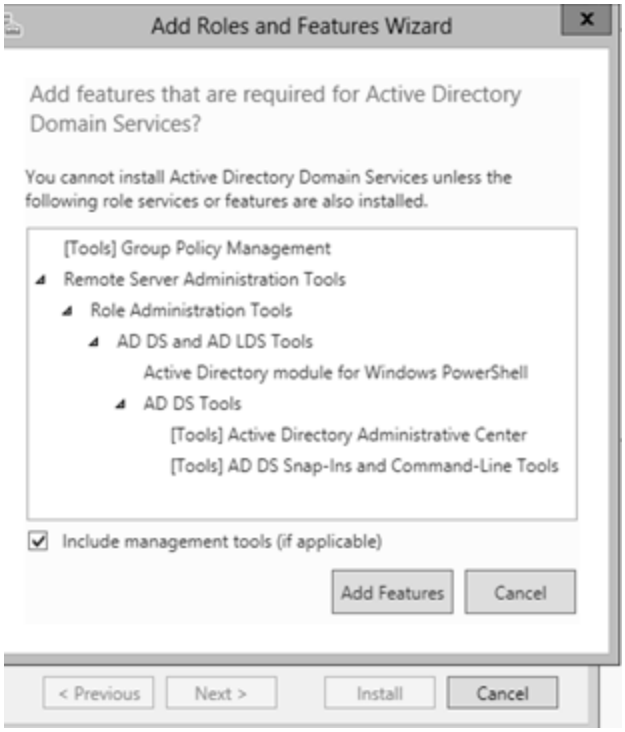
I ponownie należy kliknąć Next.



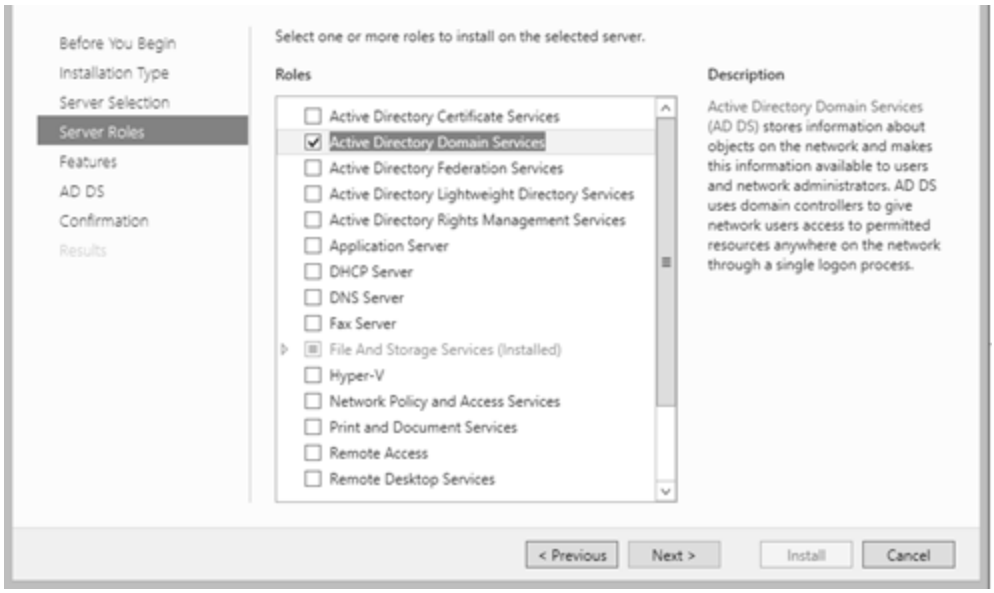
Teraz należy wybrać Serwer i kliknąć Next.



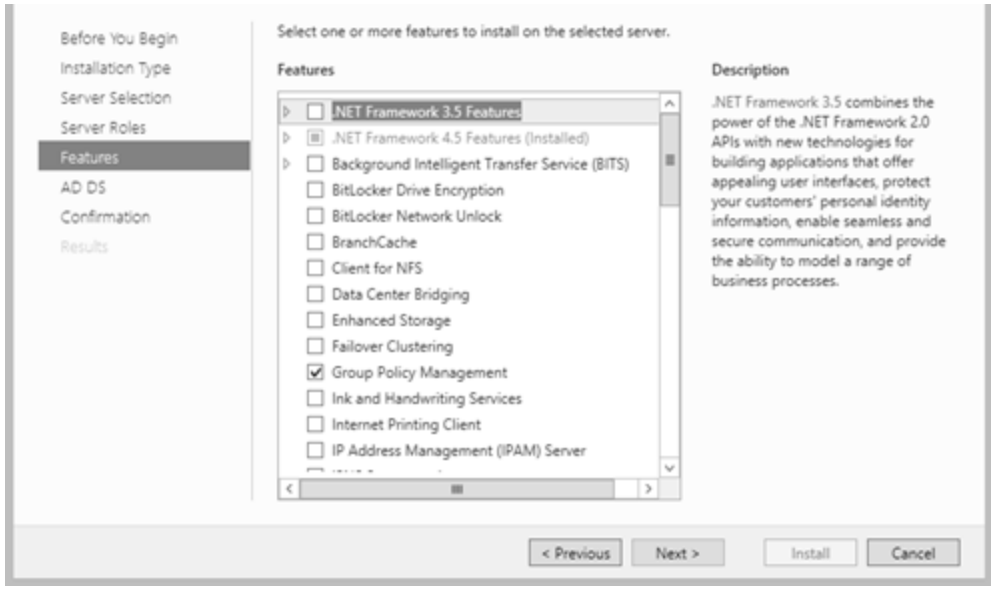
Następnie należy wybrać Active Directory Domain Services i kliknąć Add Features.



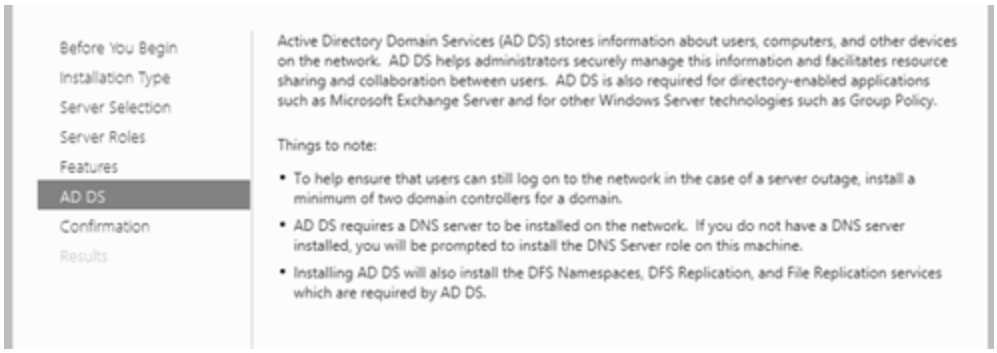
Aby przejść dalej, trzeba kliknąć Next.



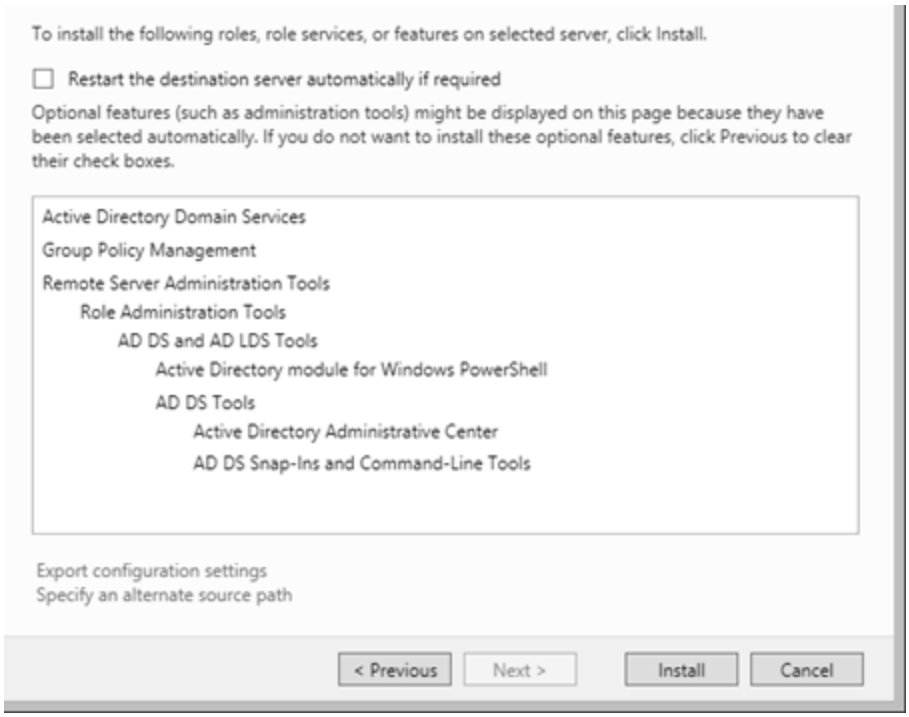
Ponownie należy kliknąć Next.



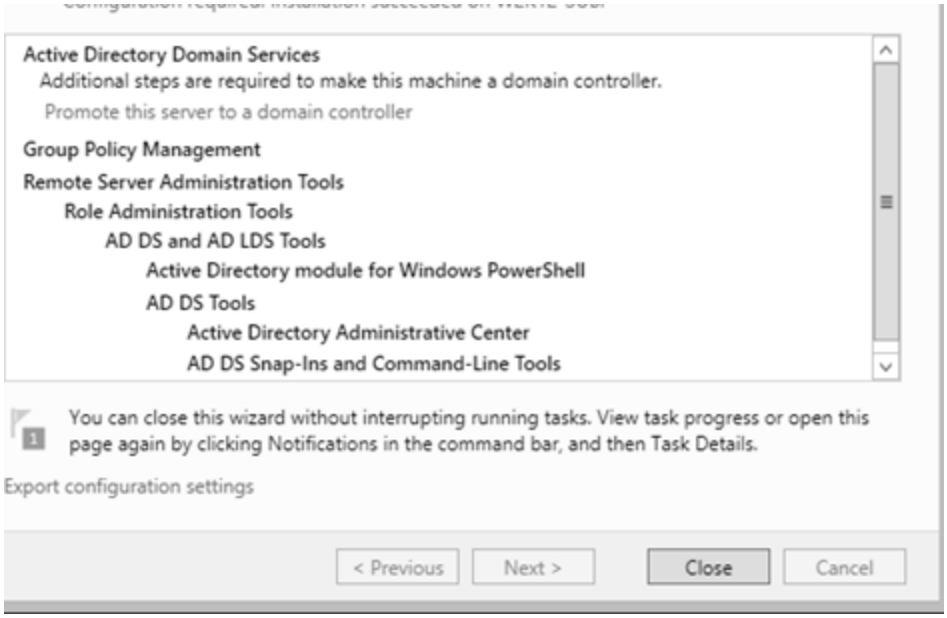
I raz jeszcze należy kliknąć Next.



Teraz wystarczy kliknąć Install.

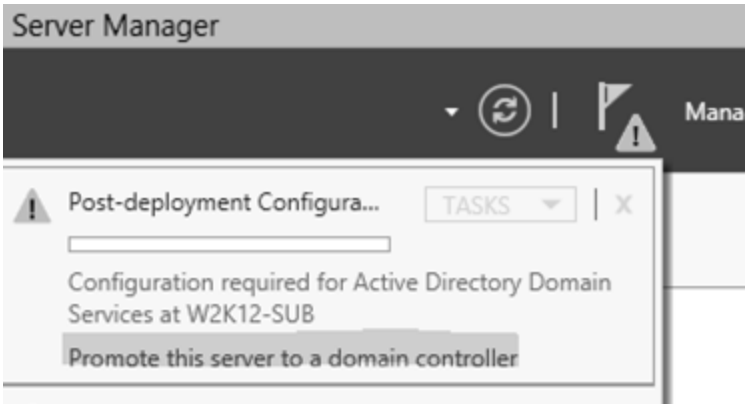


A po zakończeniu instalacji, można kliknąć Close.



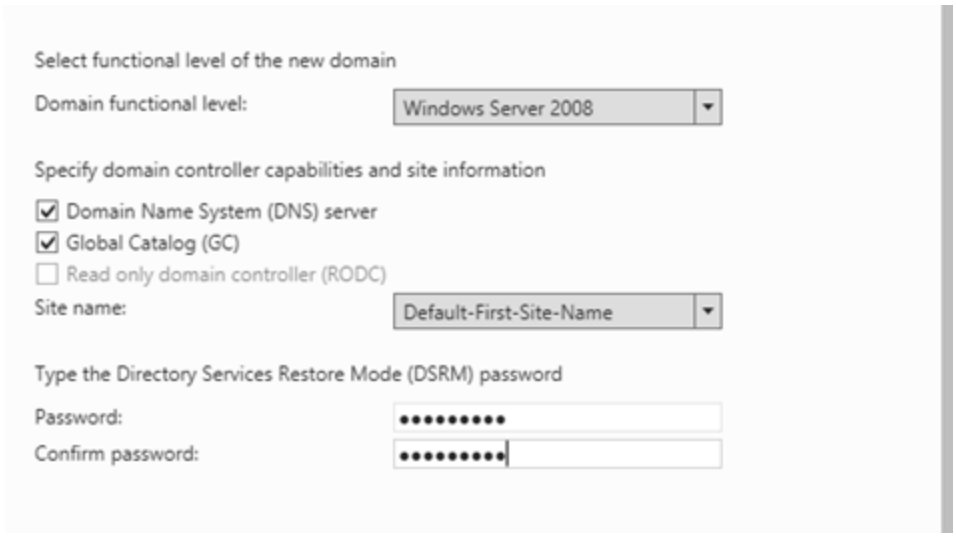
Krok 4. Promocja serwera jako kontrolera domeny

Należy kliknąć na znaku wykrzyknika na pasku powiadomień, a następnie promote this server to domain controller.

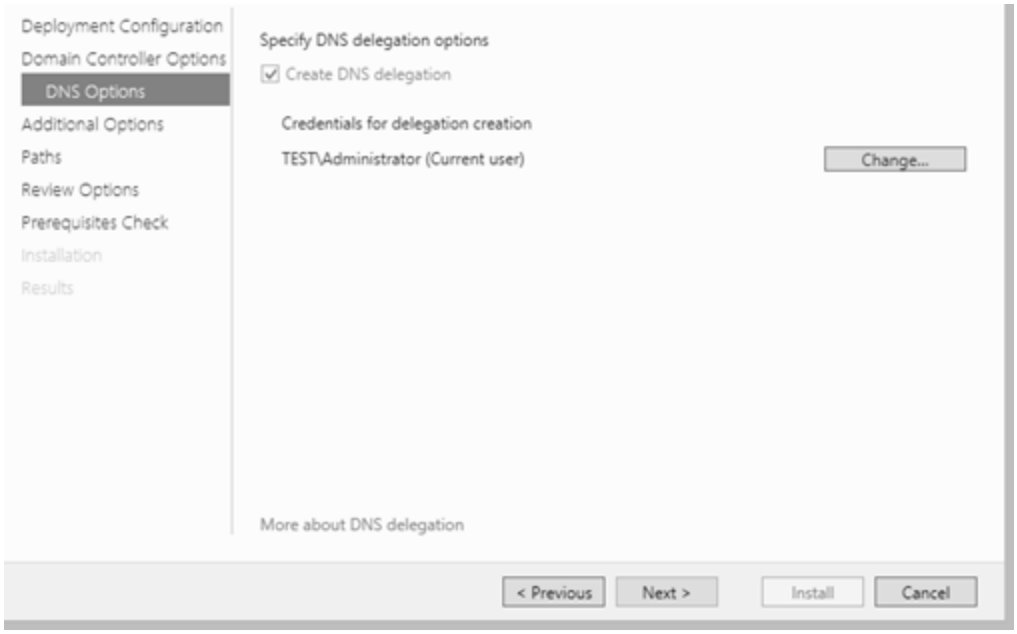


Teraz należy wybrać opcję Add a new domain to Existing Forest, a następnie wybrać typ domeny, jako domenę podrzędną (child-domain), później domenę nadrzędną i nadaćnazwę nowej domenie podrzędnej, a po wpisaniu danych należy kliknąć Next.

Teraz należy wybrać tryb Domain Functional, nazwę strony(default), podać hasło DSRM i kliknąć Next. Wybrałem Domain Functional jako 2008 ponieważ mam zróżnicowane serwery, można jednak wybrać 2016.

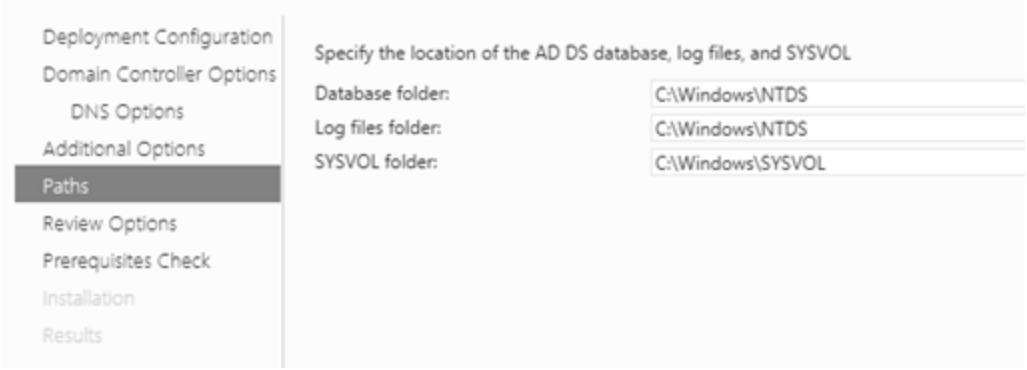


Następnie należy kliknąć Next.

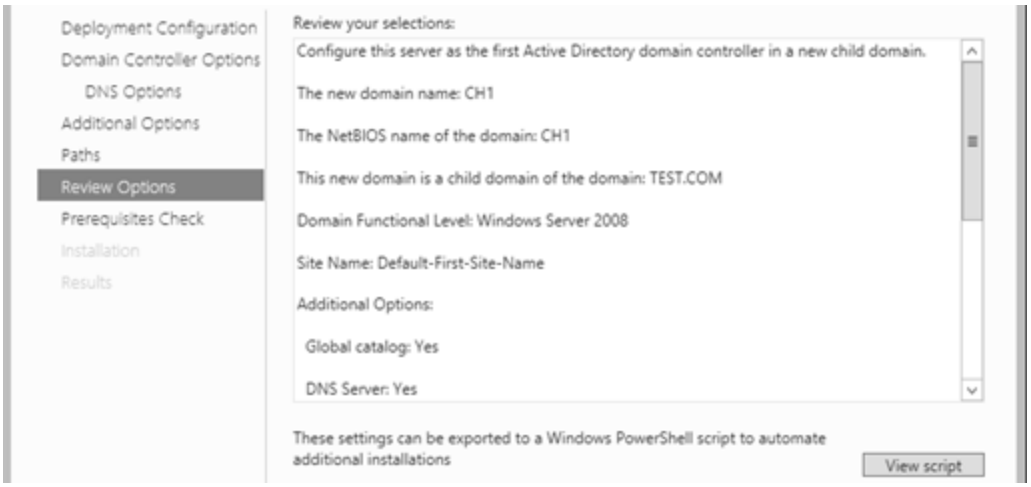


I ponownie należy kliknąć Next.

Znów należy kliknąć Next, jeżeli chcemy zachować bazową lokację lub można ją zmienić, jeżeli będzie taka potrzeba.



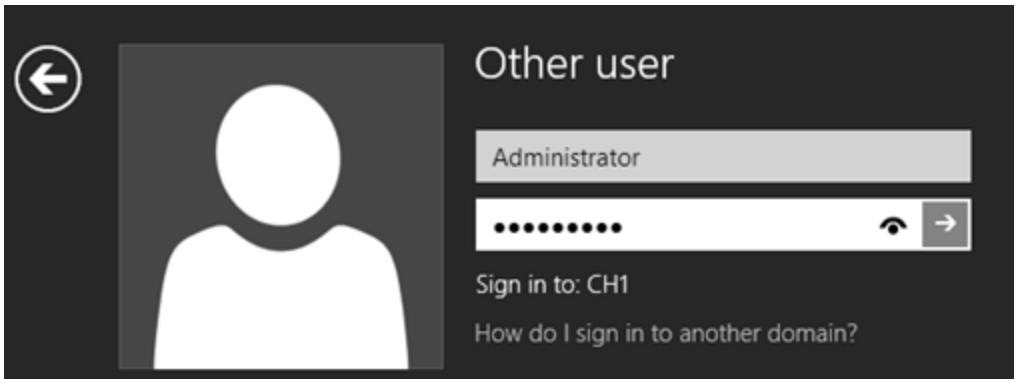
Należy kliknąć Next.



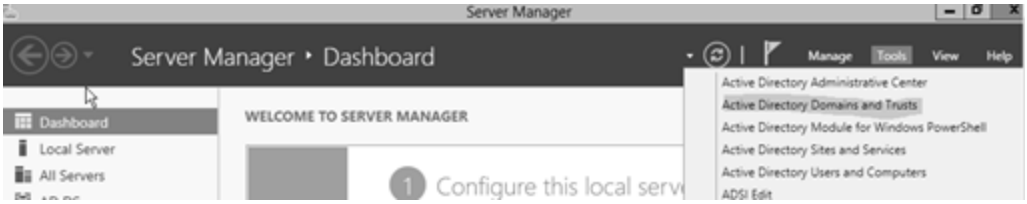
Kliknij Install, jeżeli wszystkie wymagania są spełnione.

Serwer uruchomi się ponownie automatycznie, gdy restart zostanie ukończony.

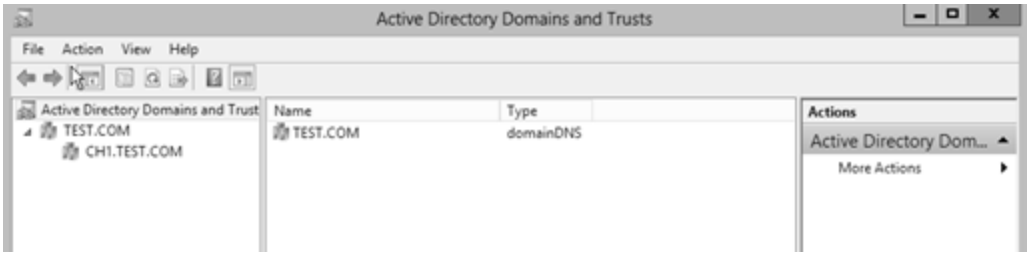
Teraz można się zalogować na serwer swoimi danymi.



Należy przejść do Active Directory Domain and Trust na nadrzędnym DC.



Teraz można zauważyć strukturę domeny, jak niżej.



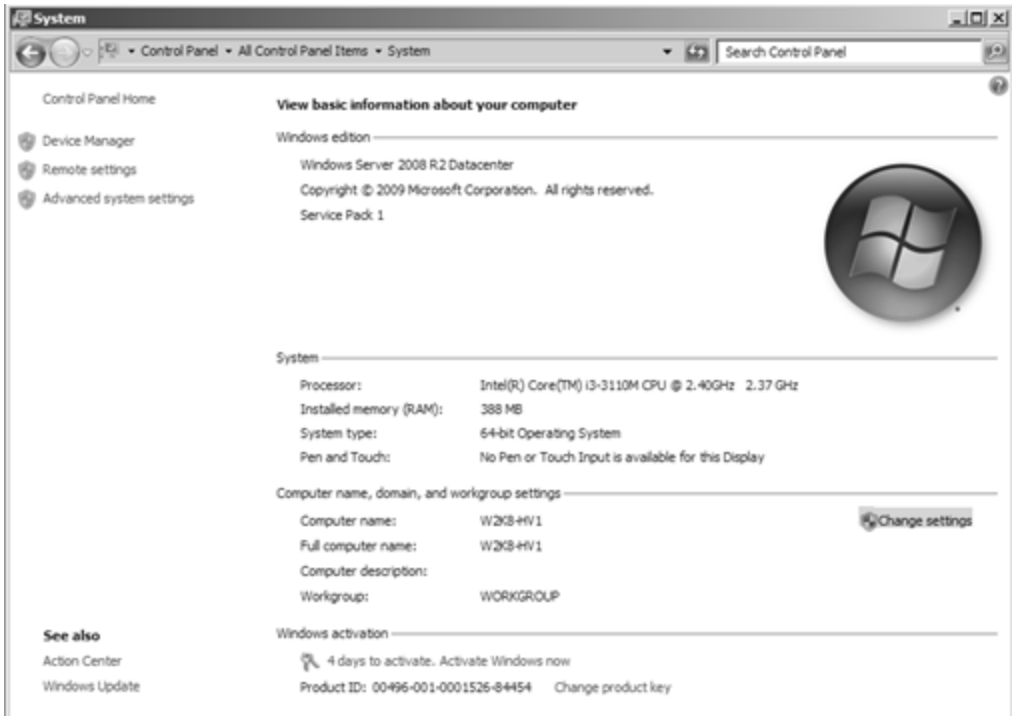
Nasza subdomena lub domena podrzędna jest aktywna.

Krok 5. Dodawanie serwera/klienta do subdomeny

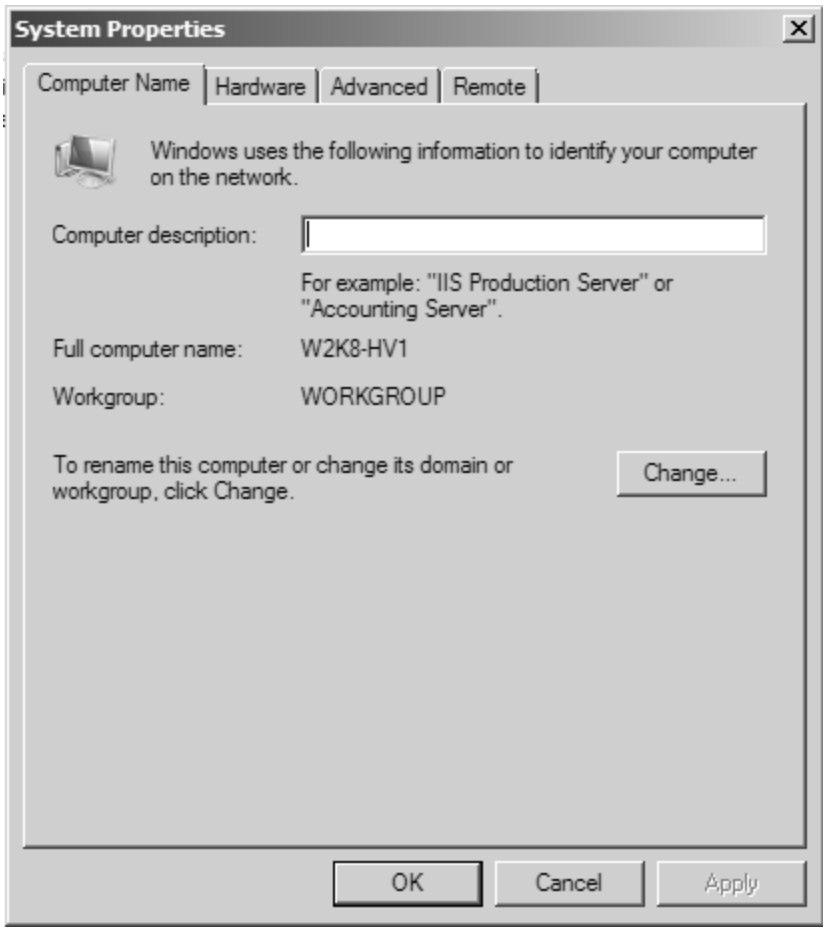
Dla celów demonstracyjnych dodam serwer Windows 2008 do domeny podrzędnej.

Należy zalogować się do serwera Windows 2008.

Następnie należy przejść do Control Panel i System i kliknąć na Change Settings.



Teraz należy kliknąć Change na System Properties.

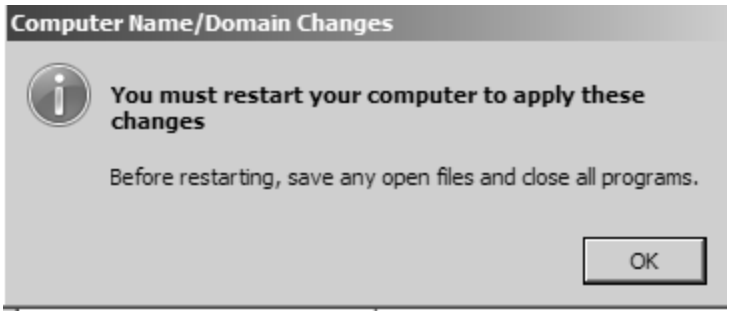


W wyznaczonym miejscu należy wpisać nazwę domeny lub subdomeny i kliknąć OK.

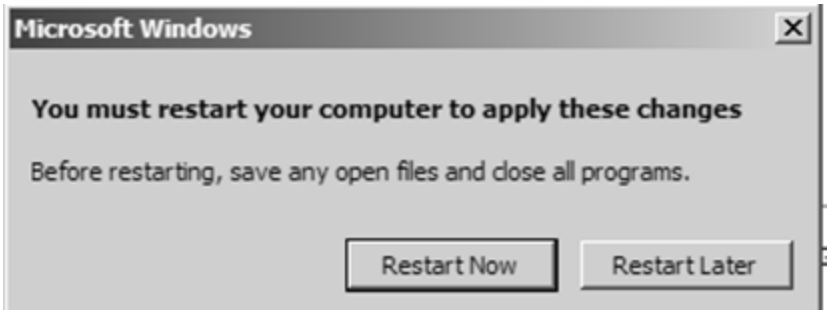
Dalej należy podać dane i kliknąć OK.

Ponownie należy kliknąć OK.

I raz jeszcze należy potwierdzić, klikając OK.

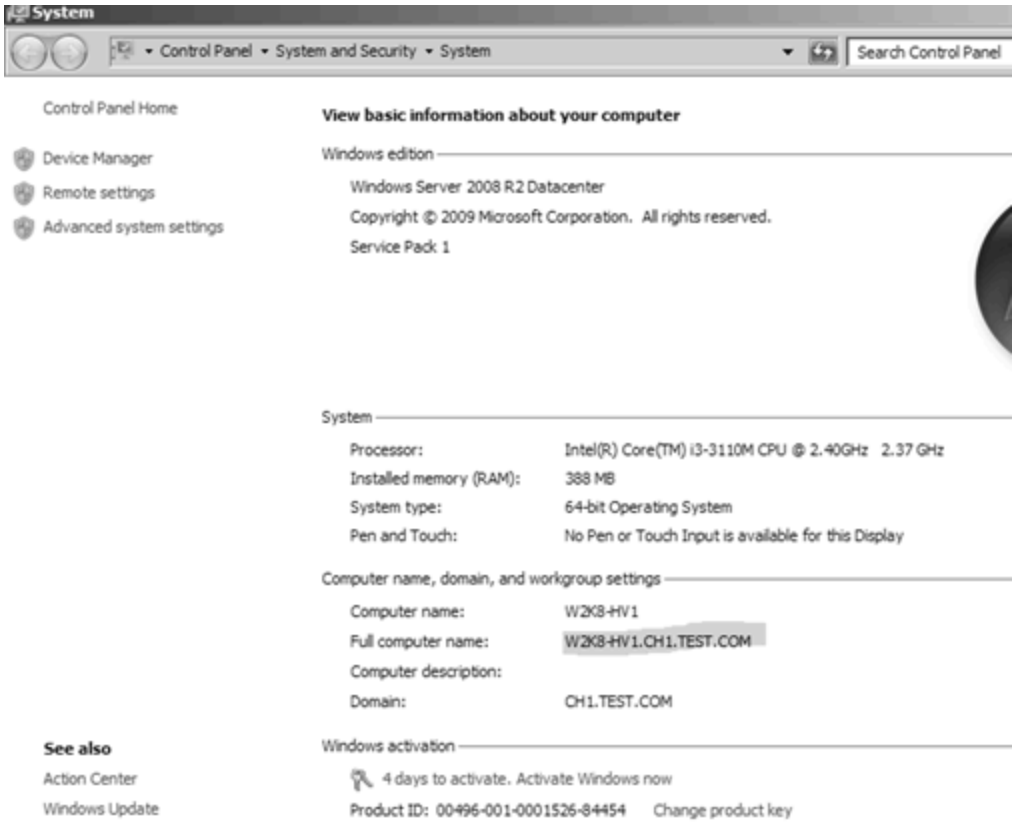


Teraz można już zamknąć System Properties i kliknąć Restart Now.



Gdy serwer uruchomi się ponownie, należy zalogować się do niego przy użyciu swoich danych.

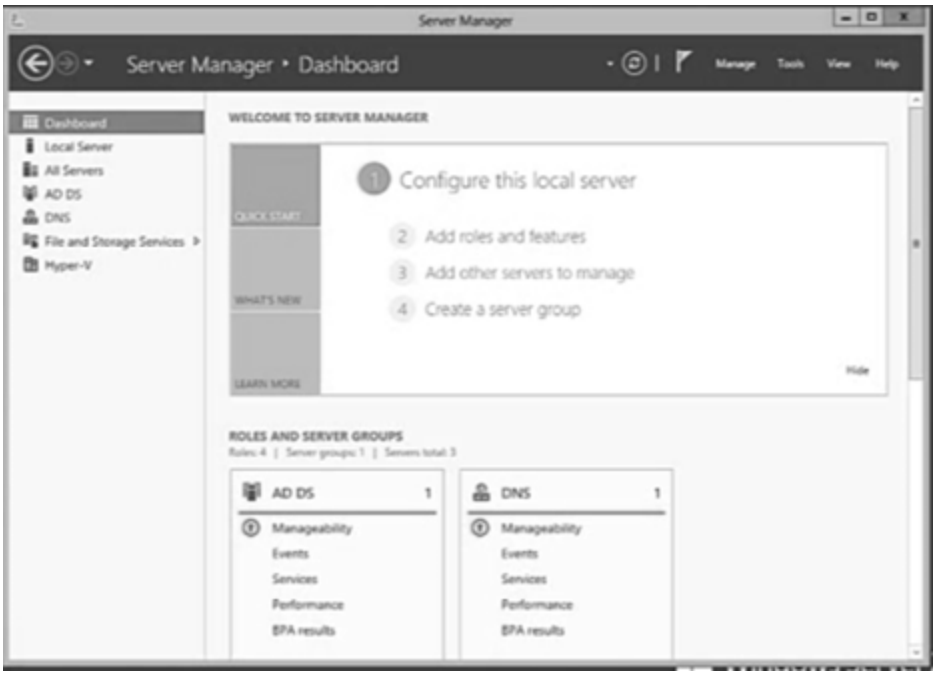
Można teraz zobaczyć, że serwer jest częścią domeny podrzędnej.



43. Klaster awaryjny Hyper-V

W mojej instalacji rola Hyper-V jest już zainstalowana na obu węzłach klastra.

Należy teraz przejść do Menedżera serwera i kliknąć Add Roles and features.



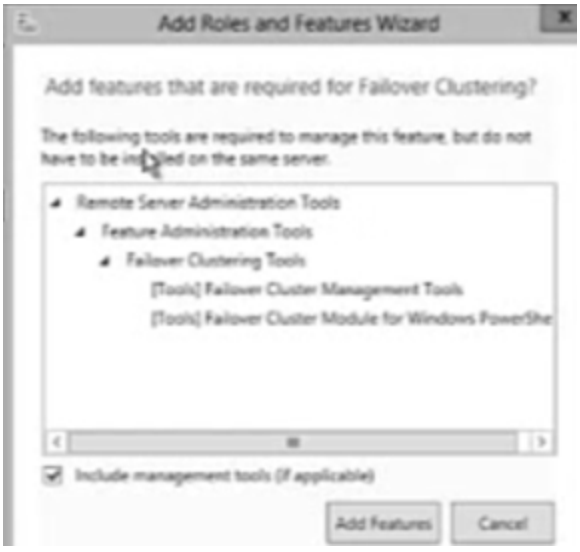
Następnie należy kliknąć Next.

Ponownie należy kliknąć Next.

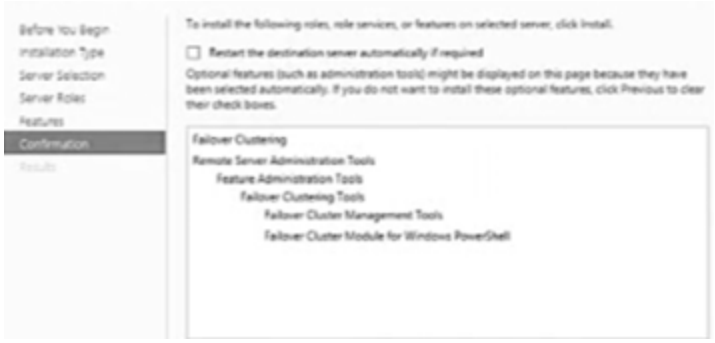
I raz jeszcze należy kliknąć Next.

Następnie należy kliknąć Failover Clustering.

Teraz trzeba kliknąć Add Features.



I można rozpocząć instalację, klikając Install.



Po zakończeniu instalacji, należy przejść do Failover Cluster Manager.

Teraz trzeba kliknąć Create Cluster.

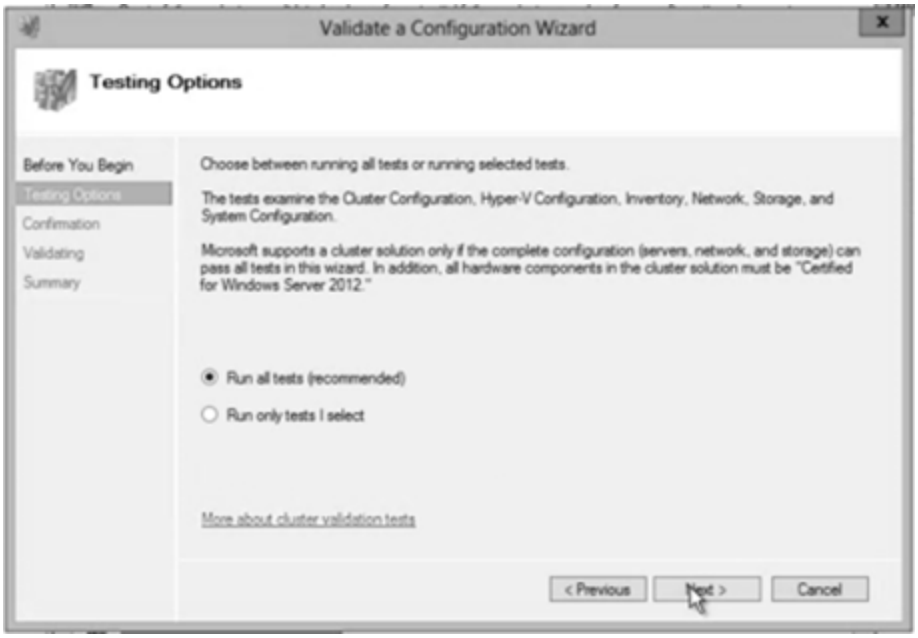
Następnie należy kliknąć Next.

Teraz można dodać węzły, które będą częścią klastra.

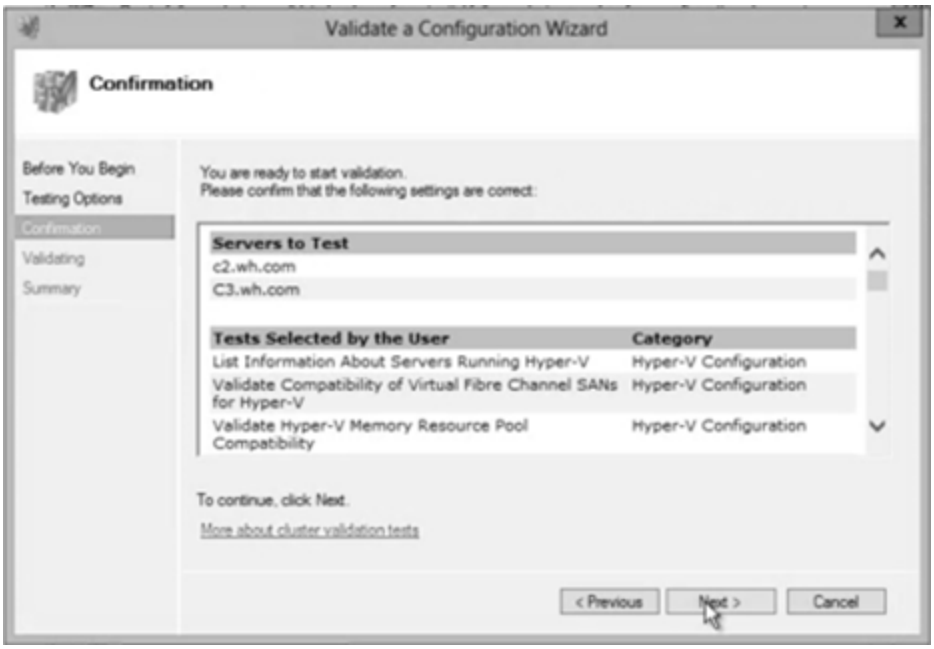
Należy wybrać Yes, aby uruchomić testy sprawdzania poprawności i kliknąć Next.

Ponownie należy kliknąć Next.

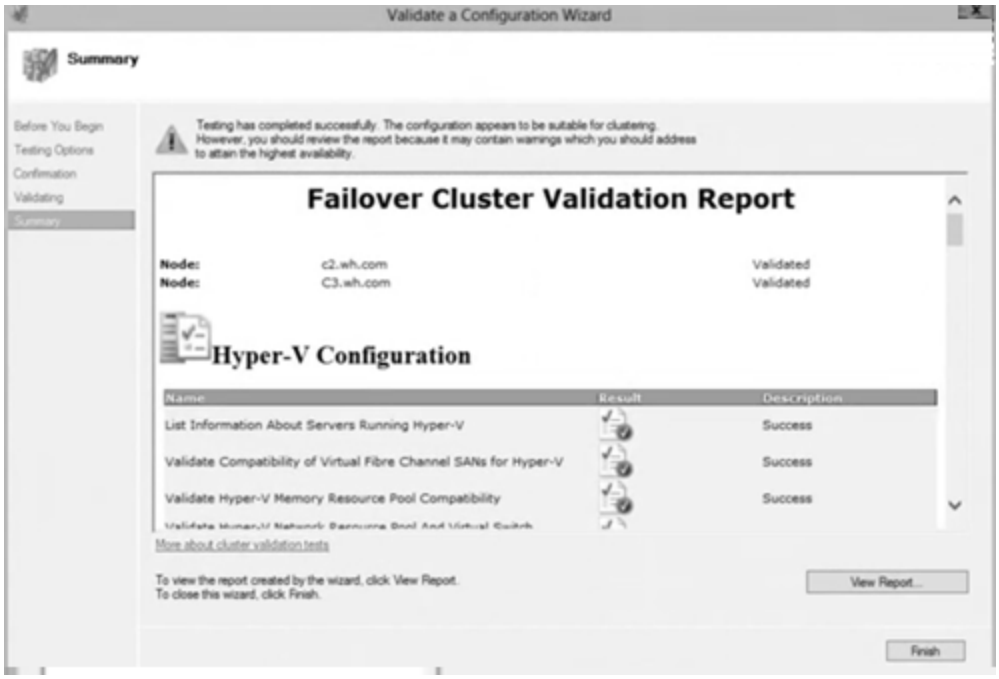
A następnie należy wybrać Run all test i kliknąć Next.



Po raz kolejny należy kliknąć Next.

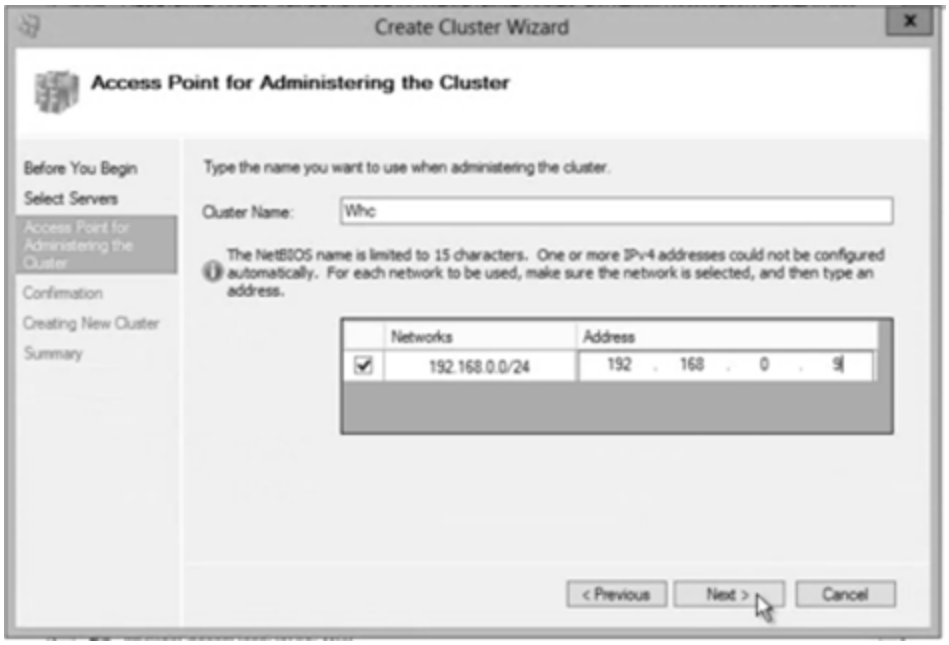


Sprawdzanie poprawności zostanie uruchomione.

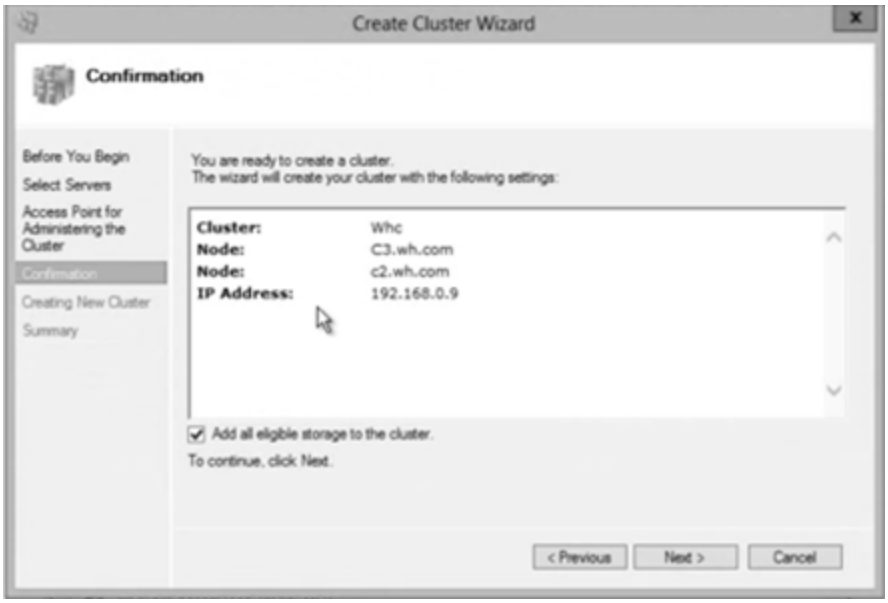


Teraz można kliknąć na View report, aby zobaczyć szczegóły raportu.

Należy podać nazwę klastra i adres IP i kliknąć Next.



Znów należy kliknąć Next.



Można zakończyć, klikając Finish.

Teraz trzeba przejść do Failover Cluster Manager.

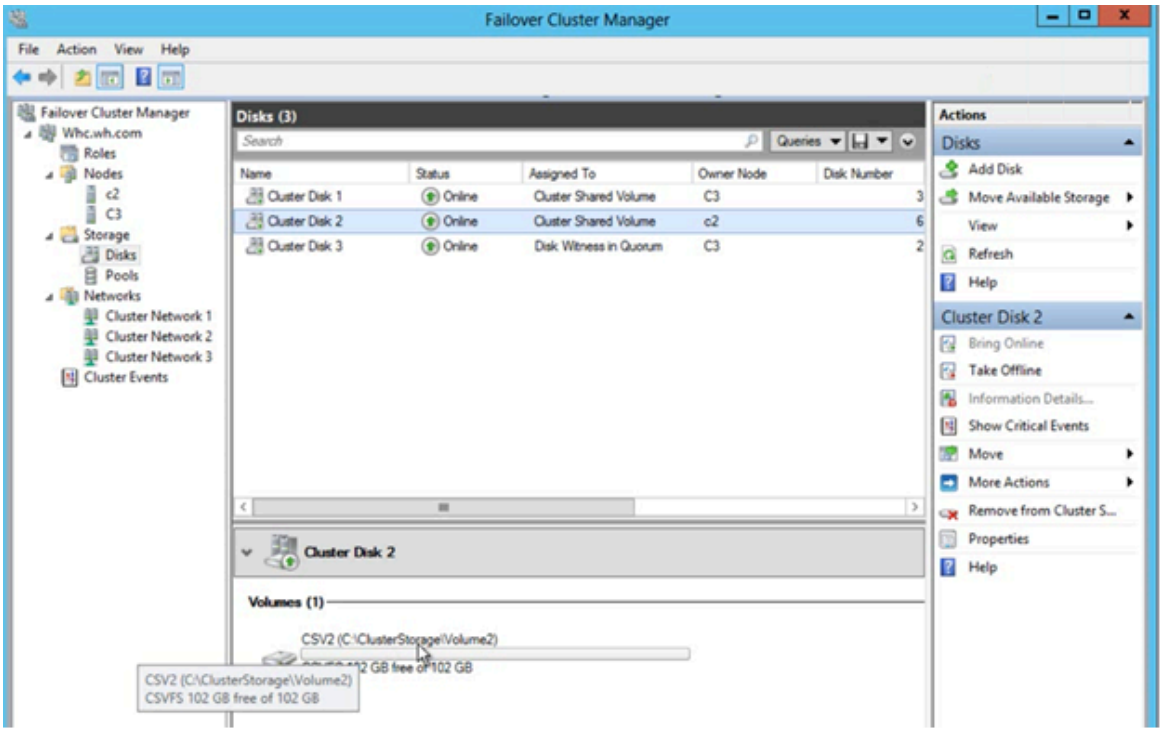
Można wyświetlić raport weryfikacji z Cluster failover Manager.

Należy rozwinąć węzły, można wówczas zobaczyć węzły, które dodaliśmy jako część klastra.

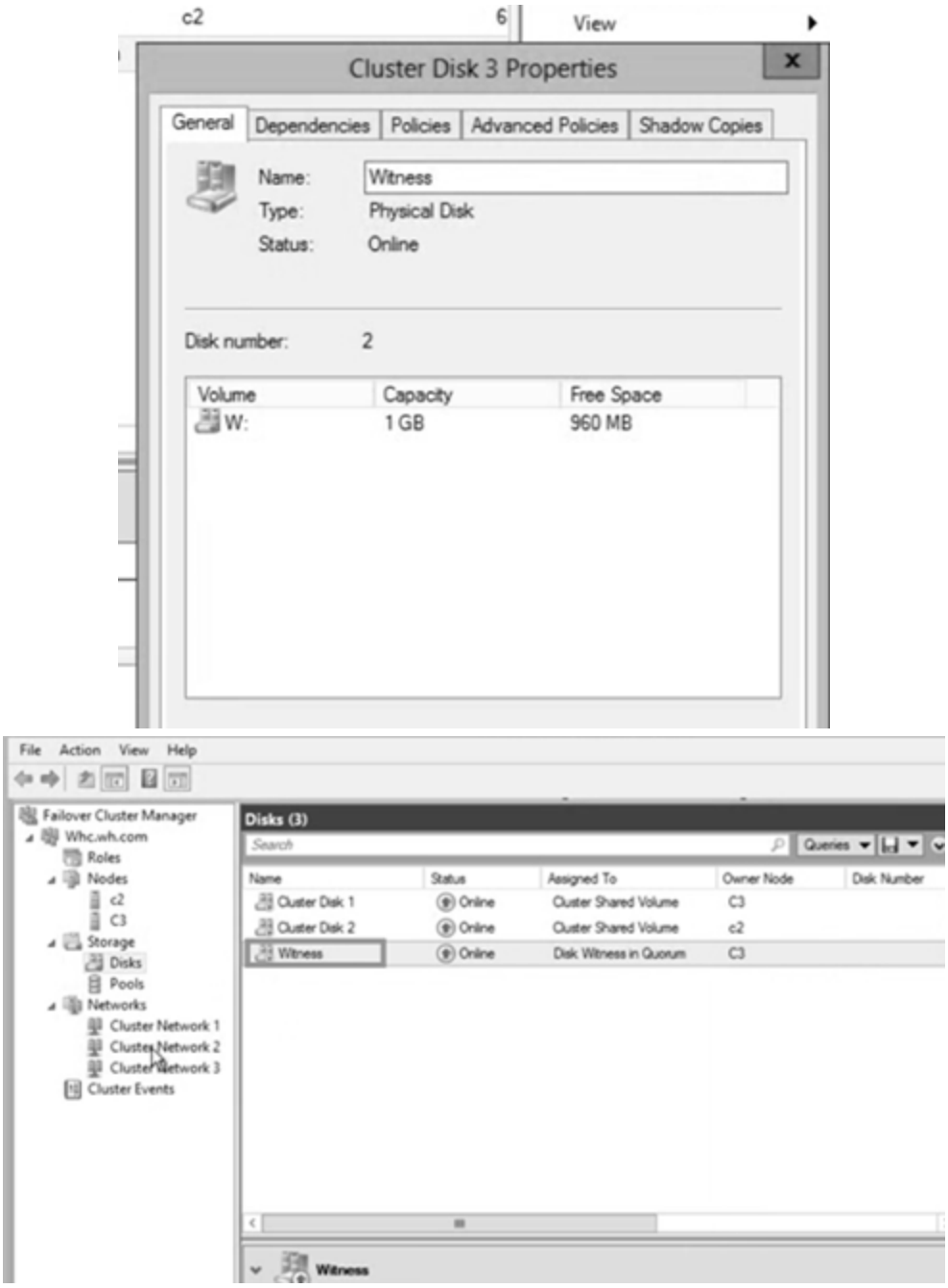
Należy kliknąć Disk, będzie można wówczas zauważyć dostępne dyski dla klastra.

Należy kliknąć prawym przyciskiem myszy na Cluster disk1 i wybrać Add to Cluster Shared Volumes.

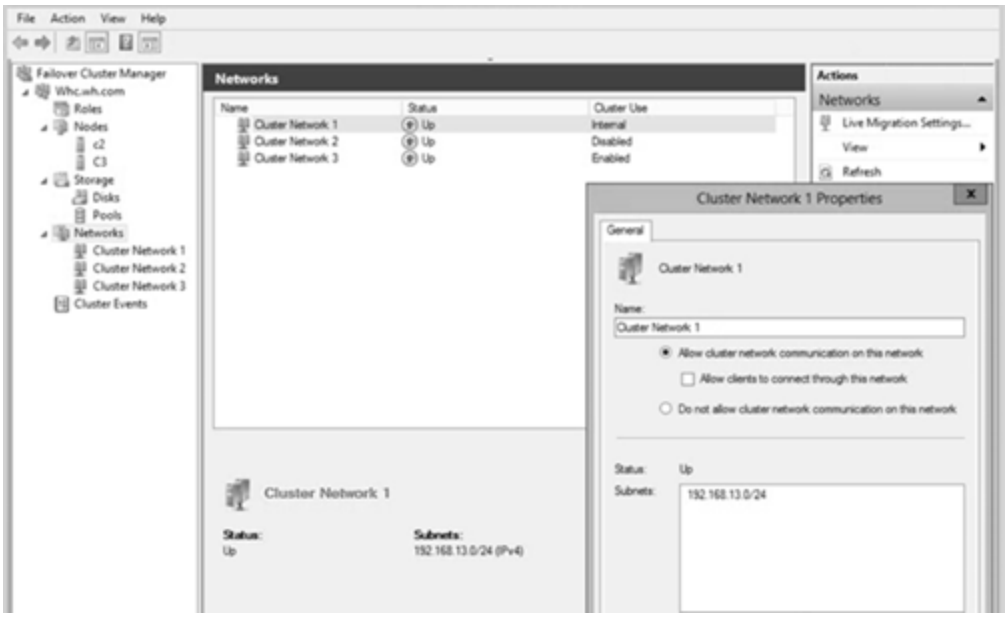
Teraz należy dodać cluster disk 2 do Cluster Shared Volumes.



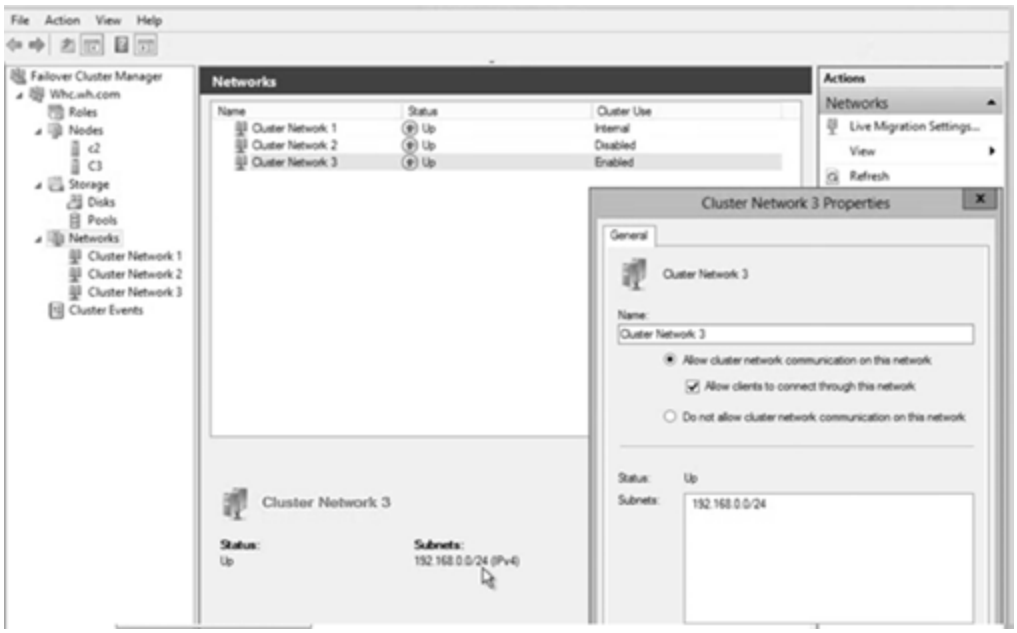
Disk 3 to dysk witness, więc należy zmienić jego nazwę na witness. Aby zmienić nazwę, wystarczy kliknąć prawym przyciskiem myszy Disk 3, przejść do properties, zaktualizować nazwę i kliknąć OK.



Można teraz zauważyć dostępne sieci klastrów. Aby skonfigurować komunikację w klastrze, należy włączyć lub wyłącz sieć. W naszym przypadku będziemy używać sieci klastra 1 i 3, a ponieważ nie będziemy używać sieci klastrów 3, wyłączymy ją. Klaster 1 będzie wewnętrzny, a klaster 3 będzie siecią publiczną.


File Action View Help
Failover Cluster Manager
Whc.wh.com
Roles
Nodes
c2
C3
Storage
Disks
Pools
Networks
Cluster Network 1
Cluster Network 2
Cluster Network 3
Cluster Events
Networks
Name
Status
Cluster Use
Cluster Network 1 Up Internal
Cluster Network 2 Up Disabled
Cluster Network 3 Up Enabled
Actions
Networks
Live Migration Settings...
View
Refresh
Cluster Network 1 Properties
General
Cluster Network 1
Name:
Cluster Network 1
Allow cluster network communication on this network
Allow clients to connect through this network
Do not allow cluster network communication on this network
Status: Up
Subnets: 192.168.13.0/24
Cluster Network 1
Status:
Up
Subnets:
192.168.13.0/24 (IPv4)

File Action View Help
Failover Cluster Manager
Whc.wh.com
Roles
Nodes
c2
C3
Storage
Disks
Pools
Networks
Cluster Network 1
Cluster Network 2
Cluster Network 3
Cluster Events
Networks
Name
Status
Cluster Use
Cluster Network 1 Up Internal
Cluster Network 2 Up Disabled
Cluster Network 3 Up Enabled
Actions
Networks
Live Migration Settings...
View
Refresh
Cluster Network 2 Properties
General
Cluster Network 2
Name:
Cluster Network 2
Allow cluster network communication on this network
Allow clients to connect through this network
Do not allow cluster network communication on this network
Status: Up
Subnets: 192.168.12.0/24
Cluster Network 2
Status:
Up
Subnets:
192.168.12.0/24 (IPv4)

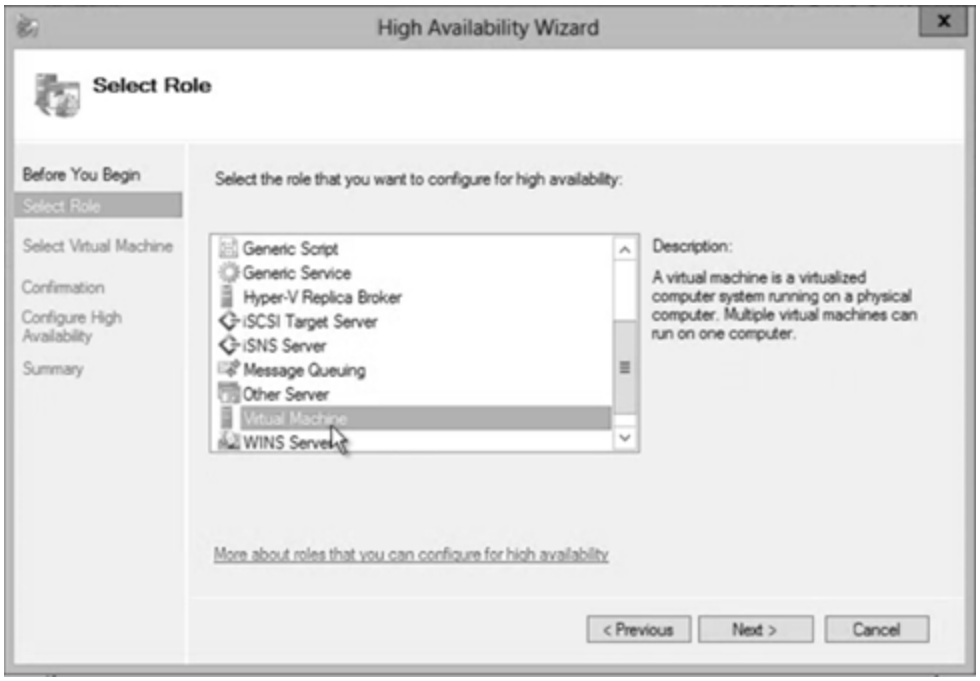


Należy ustawić kolejność sieci.

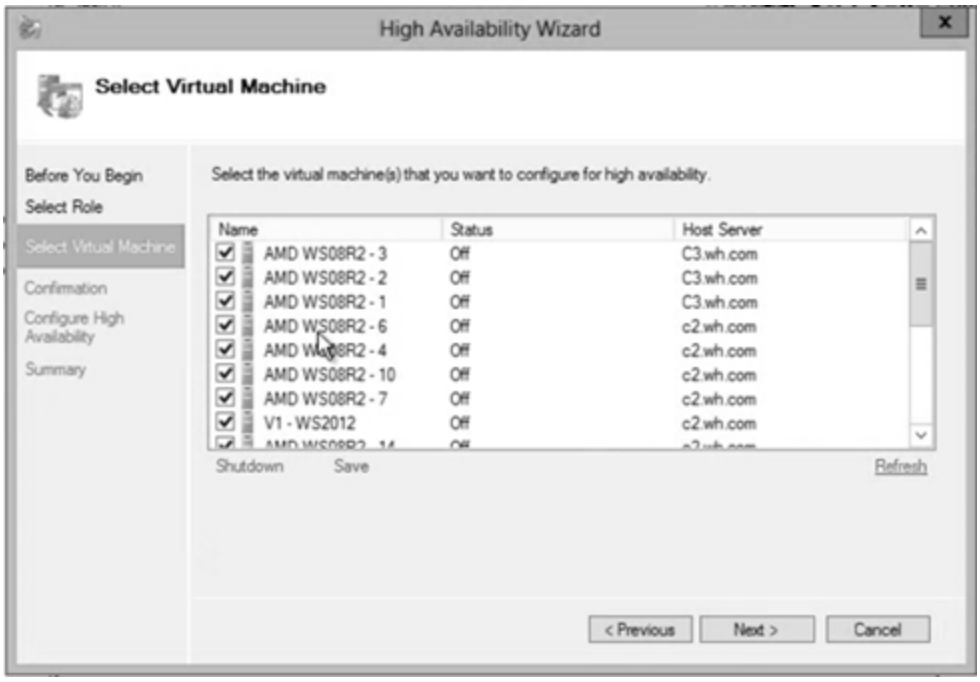
Teraz trzeba skonfigurować rolę maszyny wirtualnej w Cluster failover Manager, aby to zrobić, należy kliknąć prawym przyciskiem myszy na Roles, a następnie Configure Roles.

Dalej należy kliknąć Next.

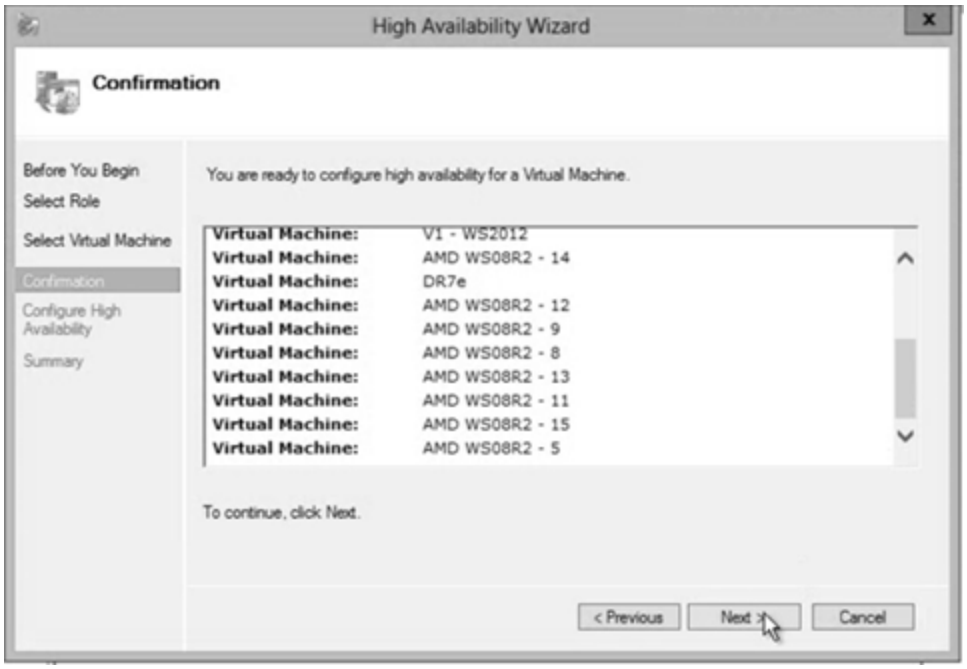
W następnym oknie należy wybrać Virtual Machine.



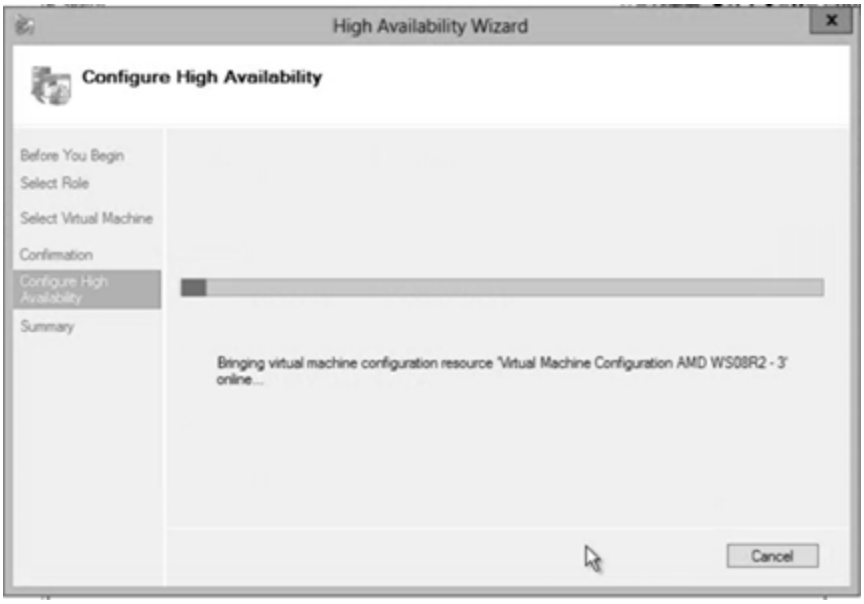
Należy dokonać wyboru maszyn wirtualnych, które chcemy skonfigurować pod kątem wysokiej dostępności. Ponieważ mamy już role Hyper-V na obu węzłach, są tu widoczne maszyny wirtualne.



Dalej należy kliknąć Next.

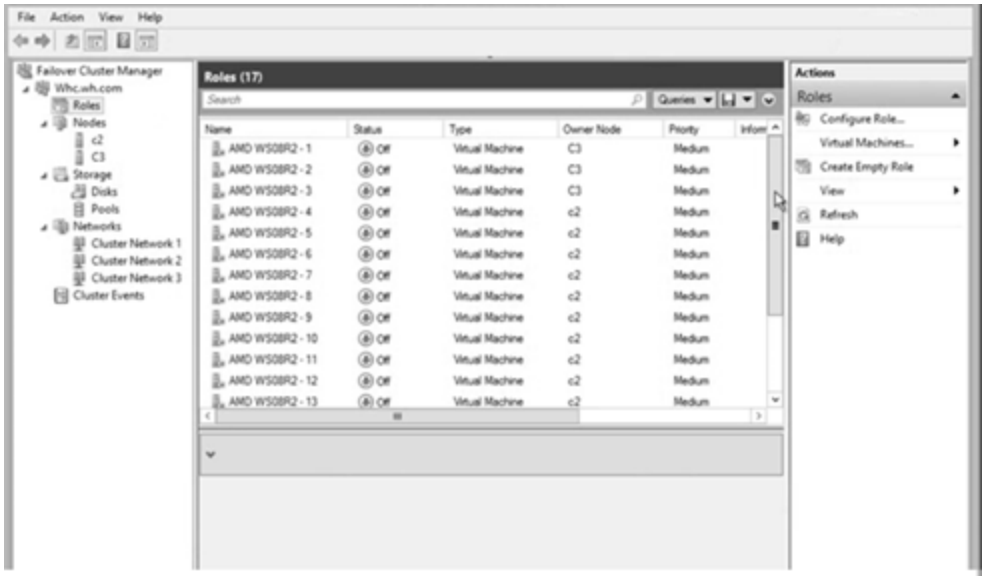


Instalator uruchomi się, aby skonfigurować wybrane maszyny wirtualne pod kątem wysokiej dostępności.

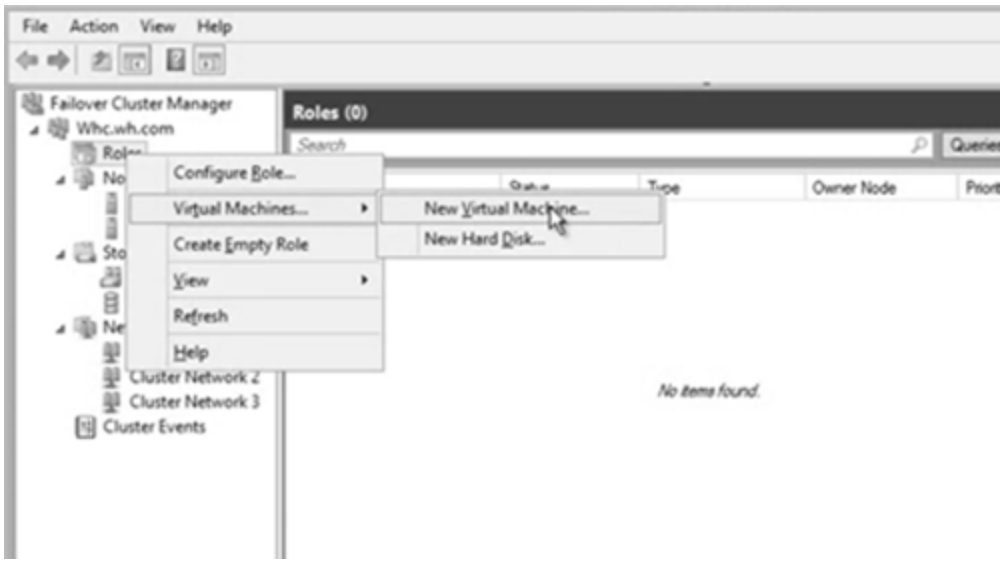


Można teraz kliknąć Finish.

Pod Roles, widoczne są teraz wszystkie dodane maszyny wirtualne.



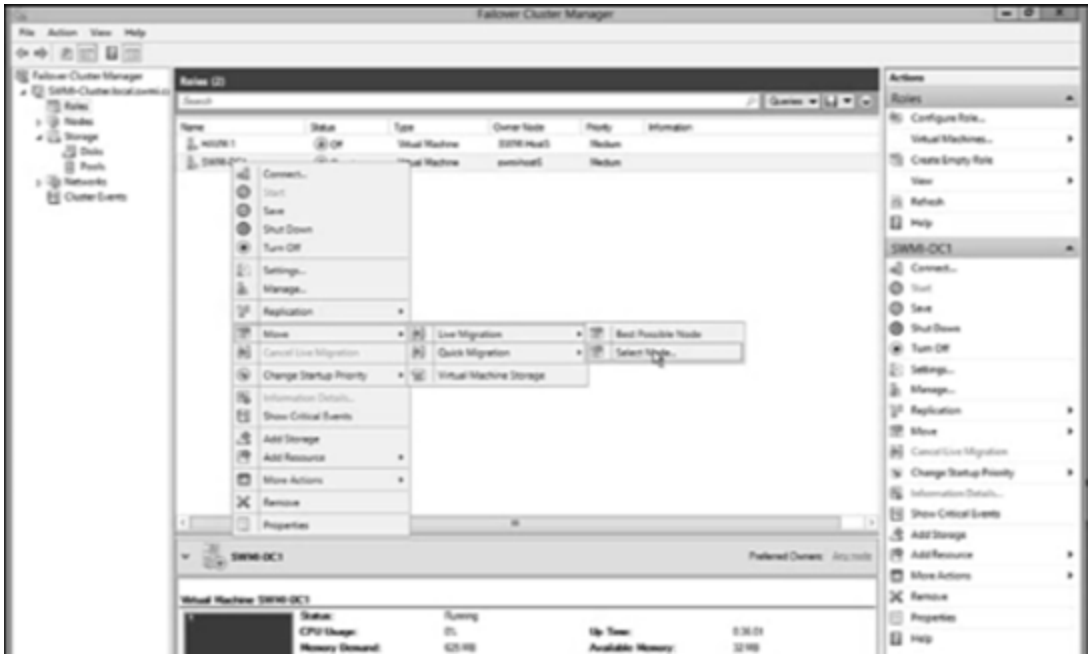
Można utworzyć wirtualną maszynę bezpośrednio tutaj. Dokładnie na Roles należy kliknąć na Virtual Machines -> New Virtual Machine.



44. Migracja na żywo w klastrze Hyper-V

W Failover cluster Manager, należy kliknąć prawym przyciskiem myszy maszynę wirtualną, którą chcemy przenieść, później kllliknąć Move a następnie wybierz Live Migration

Pod Live migration, można wybrać best possible node lub select Node. Jeżeli wybierzemy best possible, Cluster zdecyduje, gdzie zostanie zmigrowana maszyna wirtualna, jednak jeśli wiemy, gdzie należy przeprowadzić migrację, należy kliknąć drugą opcję.



Teraz należy wybrać węzeł, w którym chcemy przeprowadzić migrację i kliknąć OK.

Będzie można zauważyć postęp migracji w Failover Cluster Manager.

Po zakończeniu migracji zauważysz zauważyć będzie można, że maszyna wirtualna znajduje się na serwerze docelowym.

45. Remote FX

Funkcja RemoteFX była już obecna w Windows Server 2008 R2, jednak zapewniała znaczną poprawę w Windows Server 2016. RemoreFX VGPU to w zasadzie możliwość użycia Physical Graphic Adapter (GPU) w hoście Hyper-V do przyspieszenia renderowania treści wyświetlanych.

RemoteFX w Windows Server 2016 to zestaw ulepszeń protokołu zdalnej prezentacji Microsoft (RDP). Optymalizuje jakość wyświetlania dla użytkowników zdalnych, nawet w sieciach z ograniczeniami. Ponadto RemoteFX poprawia dostęp do urządzeń podłączonych do klienta, np. przez USB.

Funkcja vGPU w RemoteFX umożliwia wielu wirtualnym maszynom współużytkowanie fizycznej karty graficznej. Maszyny wirtualne mogą odciążać renderowanie informacji graficznych z procesora do dedykowanej karty graficznej. Zmniejszy to obciążenie procesora i poprawi skalowalność graficznych intensywnych obciążeń, które działają na wirtualnych maszynach VDI.

Wymagania:

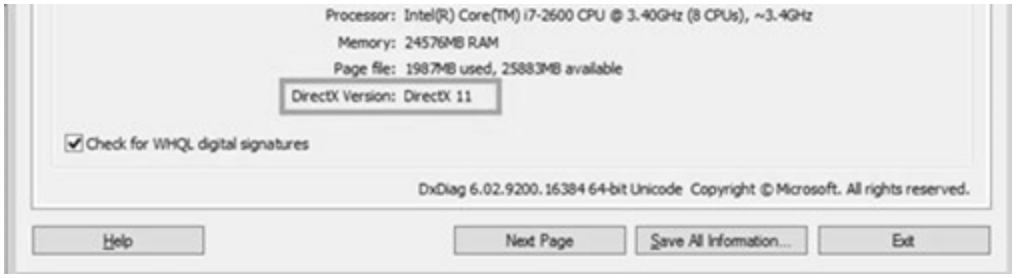
1. Procesor z obsługą SLAT.

Aby sprawdzić obsługę procesora SLAT, należy przejść do wiersza polecenia i wpisz wpisać: C:\systeminfo.exe,kliknij następnie kliknąć enter. Na końcu komunikatu będzie można zauważyć:

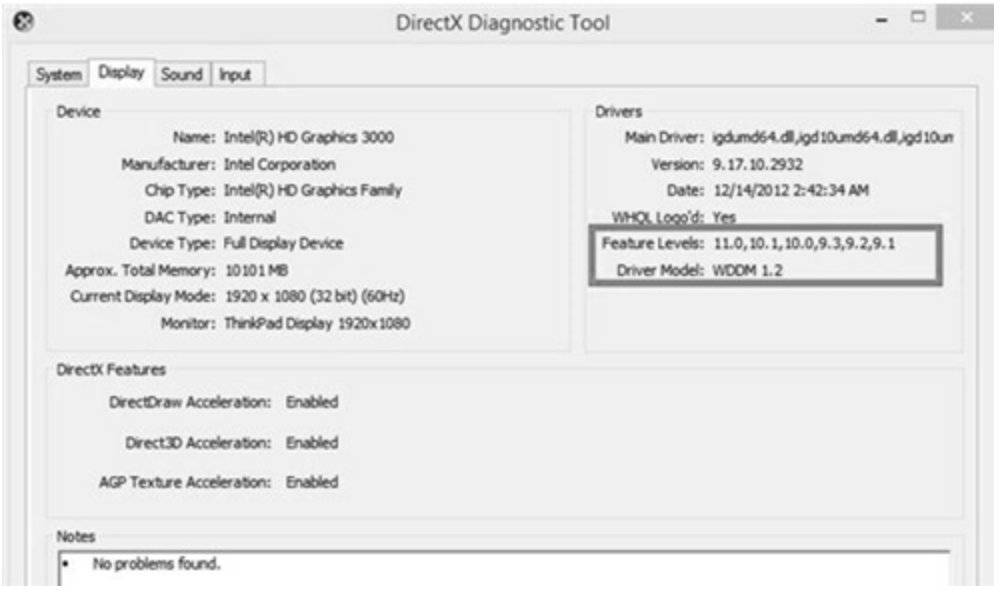
2. GPU z obsługą DirectX 11 ze sterownikiem zgodnym z WDDM 1.2.

Aby to sprawdzić, należy przejść do wiersza polecenia, wpisać c:\dxdiag.exe i kliknąć enter.

DirectX Diagnostic Tool will be displayed. Check for DirectX 11



Następnie należy przejść do Display. GPU Feature Level powienien wynosić 11, a Driver Model powienien być WDDM 1.2.



3. Windows 7 Enterprise z dodatkiem SP1 lub Windows 8 Enterprise jako system operacyjny gościa w maszynie wirtualnej z włączoną kartą wideo RemoteFX 3D.

45.1. Instalacja i konfiguracja vGPU RemoteFx

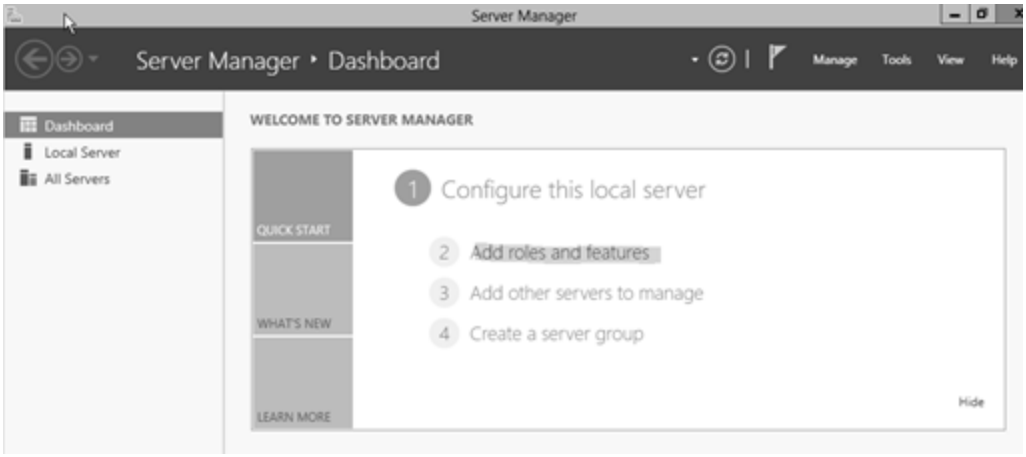
1. Należy zainstalować system Windows Server 2016.

2. Trzeba się upewnić, że na serwerze są najnowsze aktualizacje systemu operacyjnego.

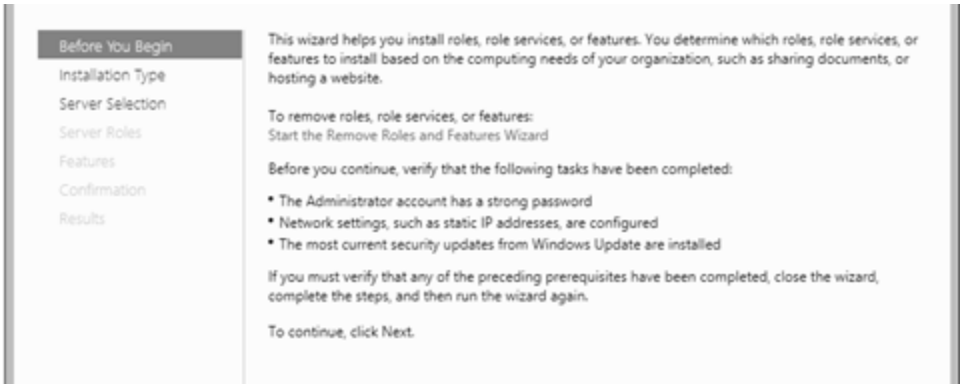
3. Należy sprawdzić, czy spełnia on wymagania podane w sekcji Wymagania.

4. Należy zainstalować Hyper-V Role i Remote Desktop Services na serwerze oraz uruchomić go ponownie.

5. Na końcu należy przejść do Server Manager i kliknąć Add Roles and Features.

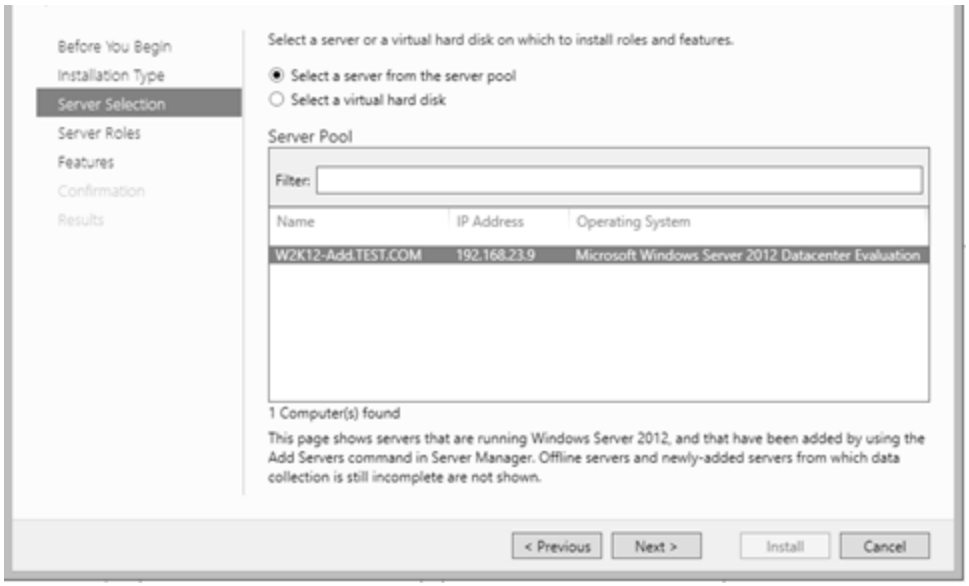


Należy kliknąć Add Roles and Features, a następnie Next.

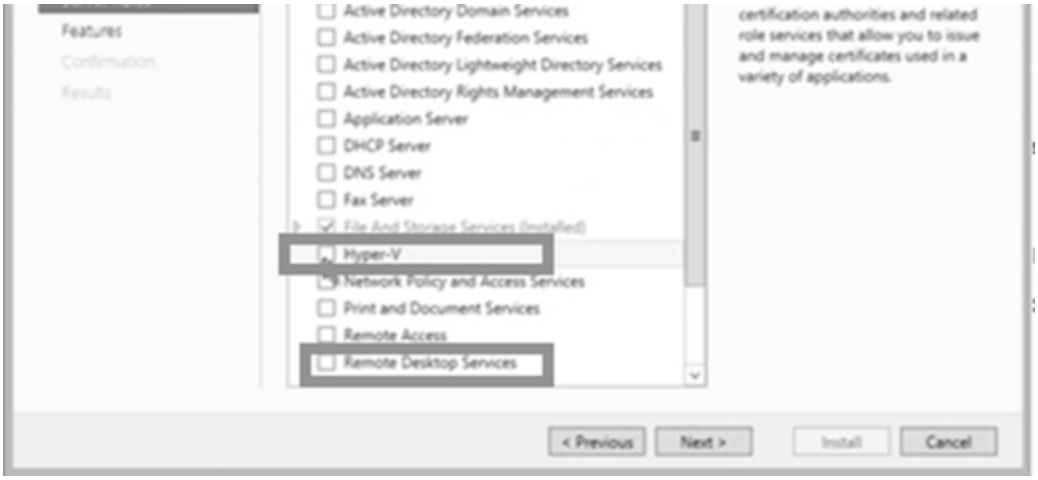


Następnie należy wybrać Role-based lub feature-based installation i kliknąć Next.

Dalej należy wybrać serwer docelowy i kliknąć Next.

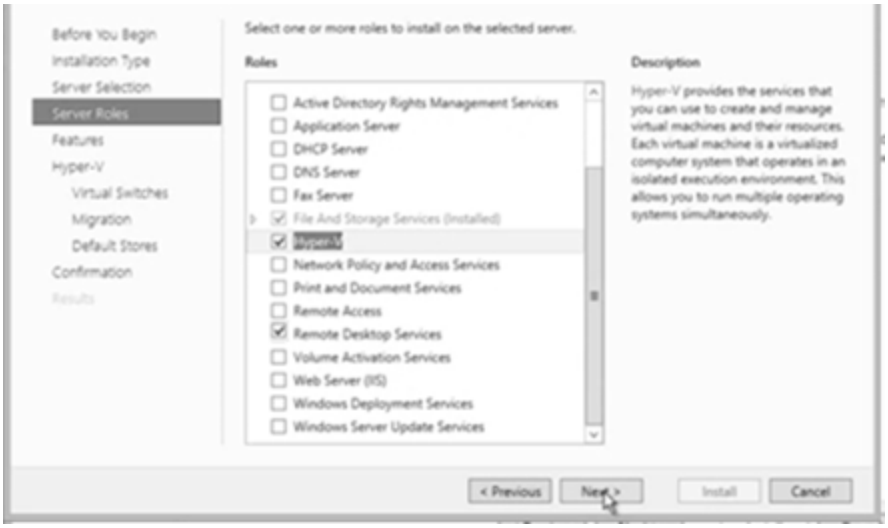


Należy wybrać Hyper-V i Remote desktop Services.



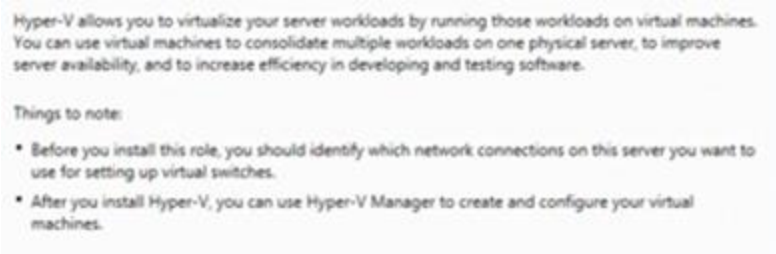
Następnie należy kliknąć Add Features.

Ponownie należy kliknąć Next.



I raz jeszcze należy kliknąć Next.

I ponownie należy kliknąć Next.



Aby przejść dalej należy wybrać kartę sieciową, za pomocą której maszyny wirtualne będą komunikować się z innymi komputerami, po czym należy kliknąć Next.

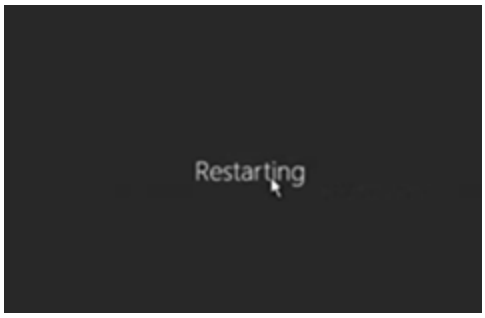
Można teraz znów kliknąć Next, gdyż skonfigurujemy opcję migracji na żywo później.

Teraz należy wybrać lokalizację, w której zostaną zapisane dyski i pliki konfiguracyjne maszyny wirtualnej i kliknąć Next.

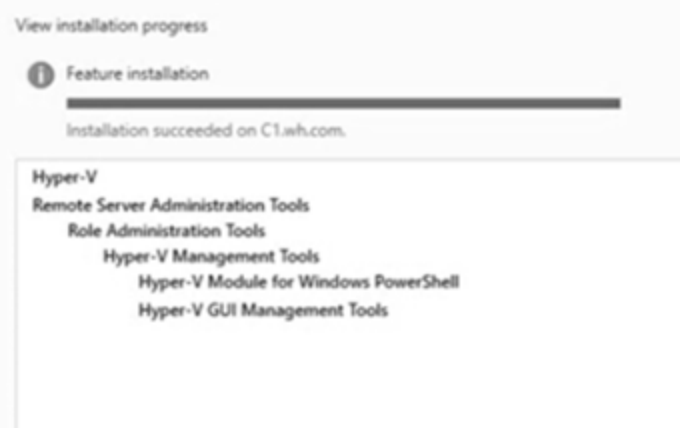
Należy zaznaczyć pole „Restart the destination server automatically if required” i kliknąć Yes, a następnie Install.

Można teraz zamknąć kreatora i obserwować postępy na pasku powiadomień.

Po zakończeniu instalacji serwer uruchomi się automatycznie.



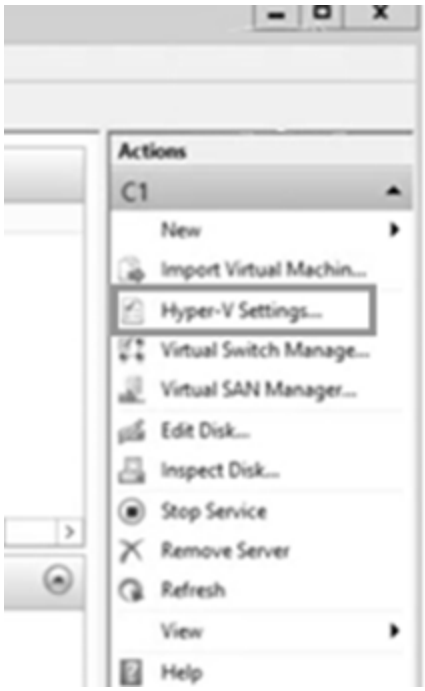
Można zamknąć kreatora.



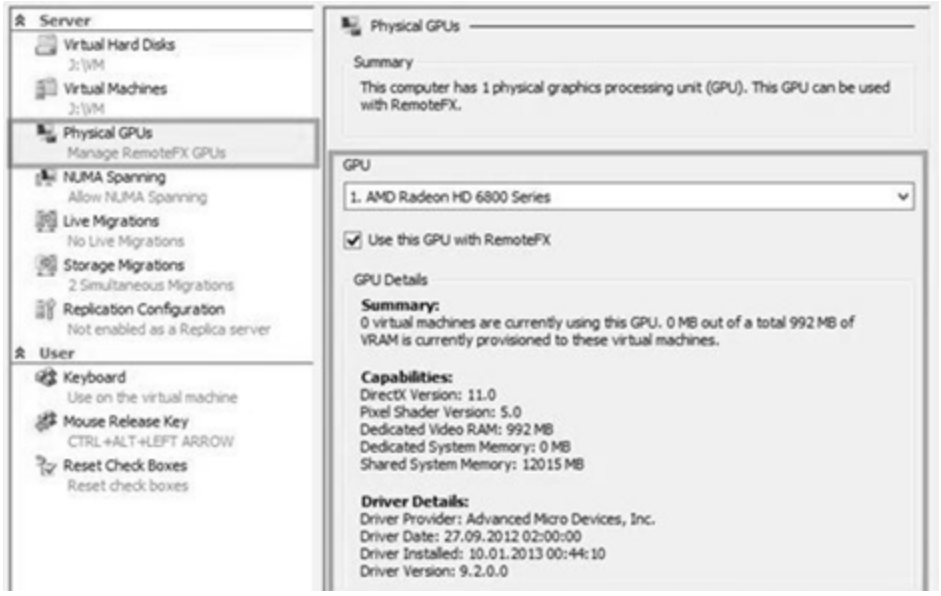
Po zakończeniu instalacji roli Hyper-V i usług pulpitu zdalnego należy uruchomić ponownie serwer.

Następnie należy przejść do Server Manager i kliknąć Hyper-V manager.

Dalej należy przejść do Hyper-V settings.

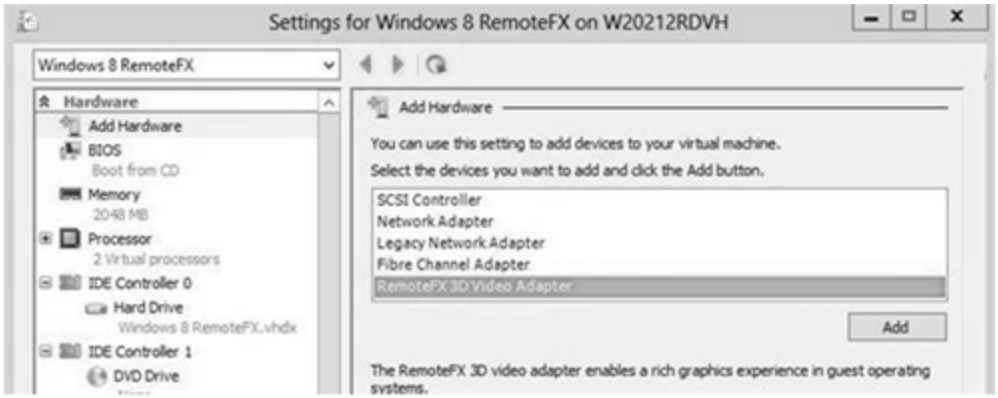


Następnie trzeba przejść do Physical GPU w ustawieniach Hyper-V.

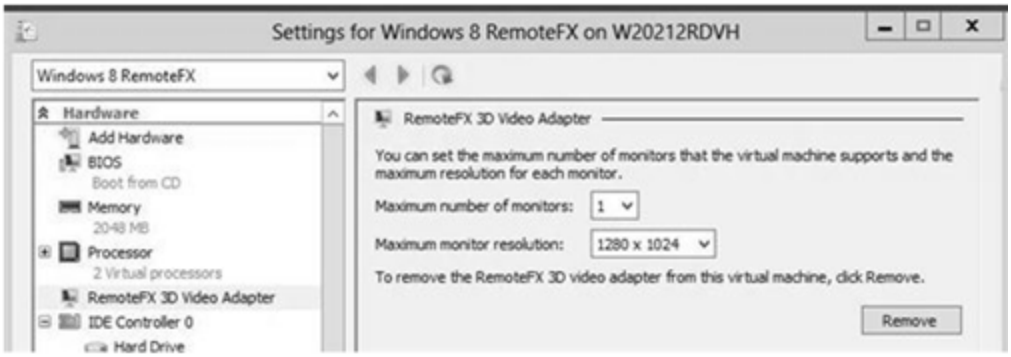


Należy dodać maszynę wirtualną Windows 8 i Windows 7 na Windows Server 2016 i przejść do ustawień tej maszyny wirtualnej.

Na settings należy kliknąć add hardware i wybrać Remote 3D Video Adapter, a następnie kliknąć add.



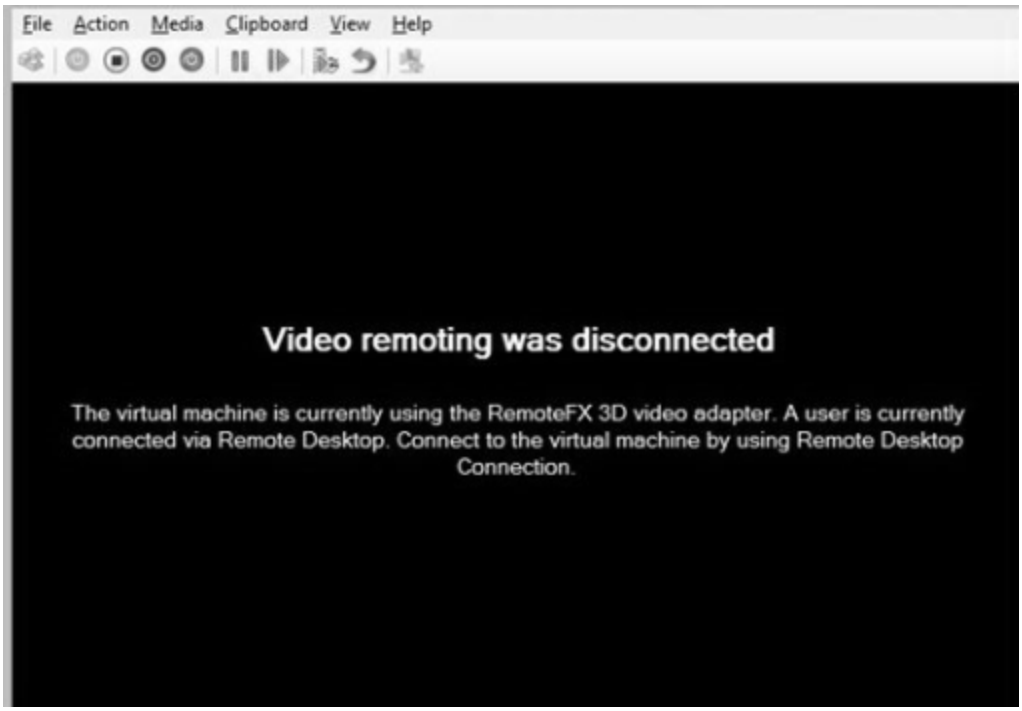
Dalej należy przejść do nowo dodanego RemoteFx 3D Video Adapter oraz skonfigurować maksymalną liczbę monitorów i maksymalną rozdzielczość monitora używaną przez klienta.



Teraz należy zapisać zmiany i uruchomić maszynę wirtualną.

Korzystając z Podłączania pulpitu zdalnego, należy zmienić Performance Experience na LAN. Umożliwia to prawidłowe działanie adaptera RemoteFX na maszynie wirtualnej.

Po ponownym uruchomieniu maszyny wirtualnej wyświetli się komunikat o błędzie na ekranie. To normalne i nie będzie można wówczas zalogować się do maszyny wirtualnej z połączenia maszyny wirtualnej. Będzie można zdalnie logować się do maszyny wirtualnej za pomocą konta należącego do grupy Użytkownicy pulpitu zdalnego na maszynie wirtualnej.



46. Relacja zaufania pomiędzy domenami

Głównym powodem istnienia Active Directory jest uwierzytelnienie obiektów (np. użytkowników, komputerów) i autoryzacja (lub jej odmowa) dostępu do innych obiektów Active Directory (dowolnych, np. kontenera lub obiektu użytkownika) oraz do zasobów innych, w tym dyskowych, sieciowych oraz aplikacji. Żeby była możliwa automatyczna autoryzacja użytkownika wobec innej usługi Active Directory lub zasobów korzystających z tej innej usługi (np. zasobu sieciowego), musi istnieć relacja zaufania pomiędzy domenami Active Directory.

Domeny połączone relacją zaufania „ufają sobie”, o ile jest to relacja zaufania dwustronna, lub tylko „jedna ufa drugiej”, jeżeli jest to relacja jednostronna. Domeny w obrębie jednego lasu (w tym w obrębie tego samego drzewa) ufają sobie.

Do celów demonstracyjnych stworzyłem dwa lasy z domenami TEST.COM i LAB.COM.

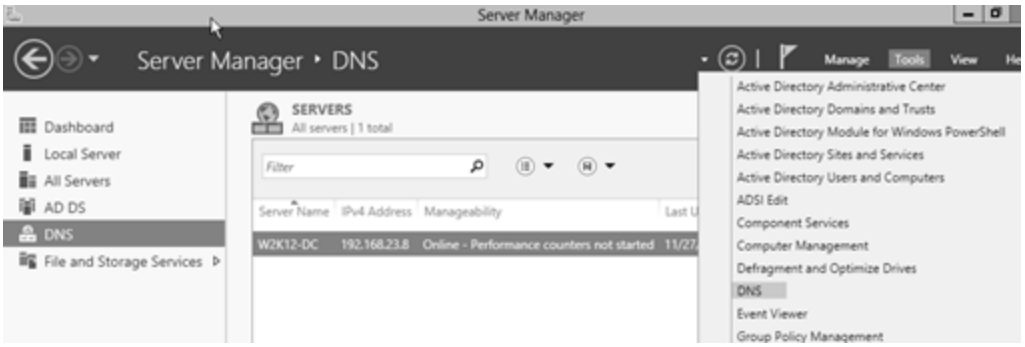
Poniżej przedstawiono kroki, które należy wykonać, aby utworzyć relację zaufania na poziomie lasu i domeny.

Wymagania wstępne

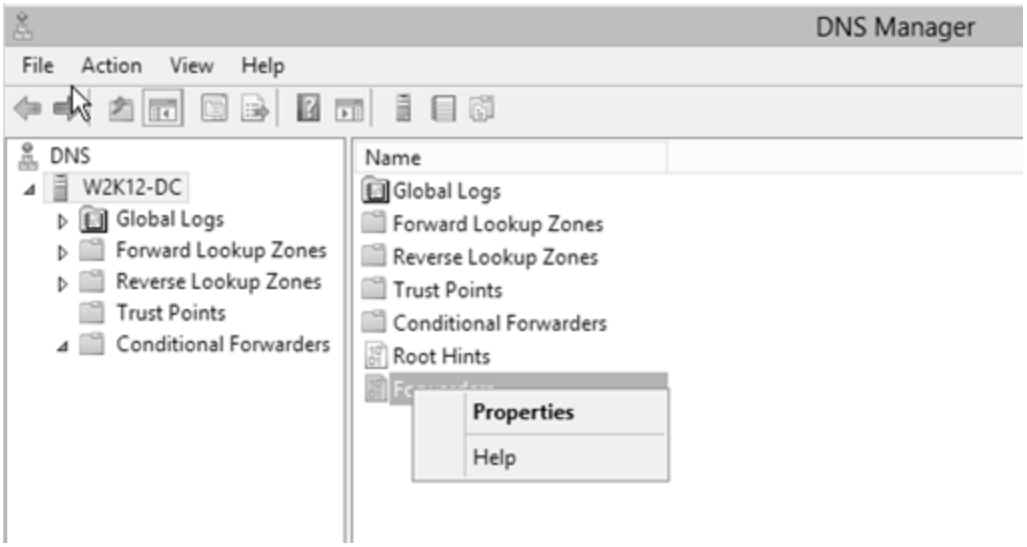
1. Tworzenie przekazywarki DNS

Należy zalogować się do serwera DNS w TEST.COM. W naszym przypadku mamy również DC jako serwer DNS. Tak więc zaloguję się do mojego DC, W2K12-DC.

Następnie należy przejść do DNS Console z Tools Menu na Server Manager.

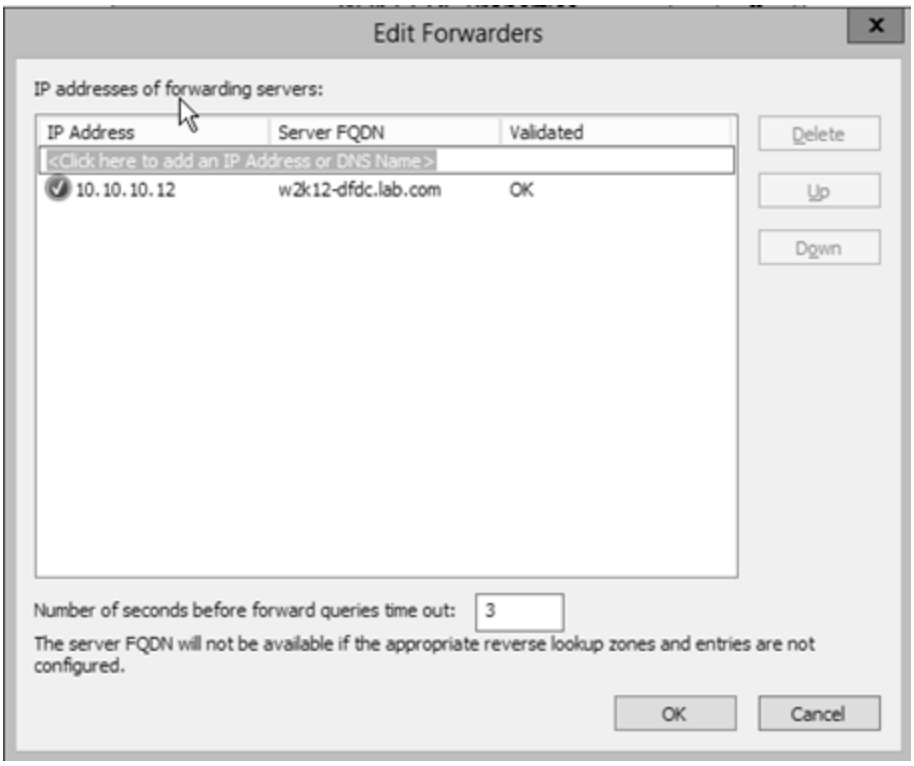


Na konsoli DNS należy kliknąć prawym przyciskiem myszy Forwarder i przejść do properties.



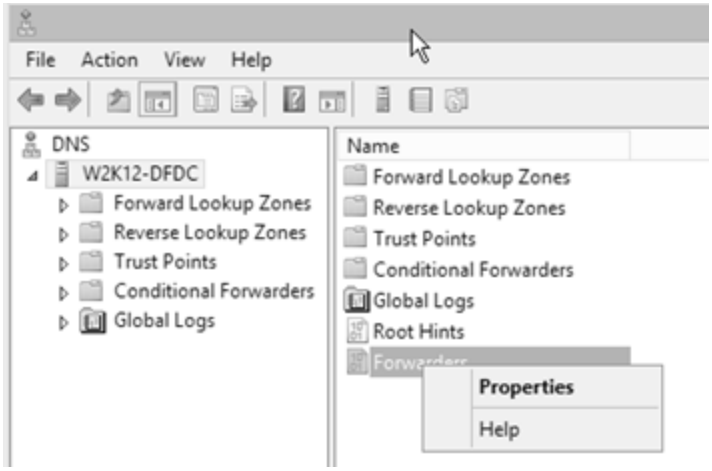
Na zakładce Forwarders należy kliknąć Edit.

Dalej należy wpisać adres IP innej domeny DNS i nacisnąć Enter i kliknąć OK.

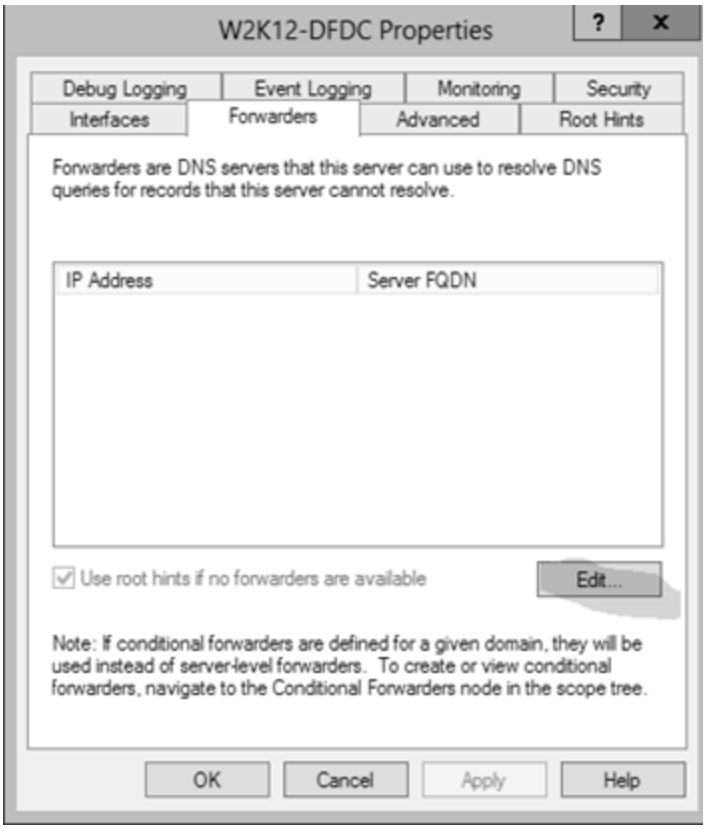


Teraz należy kliknąć Apply i OK (weryfikacja nazwy FQDN serwera zajmie trochę czasu).

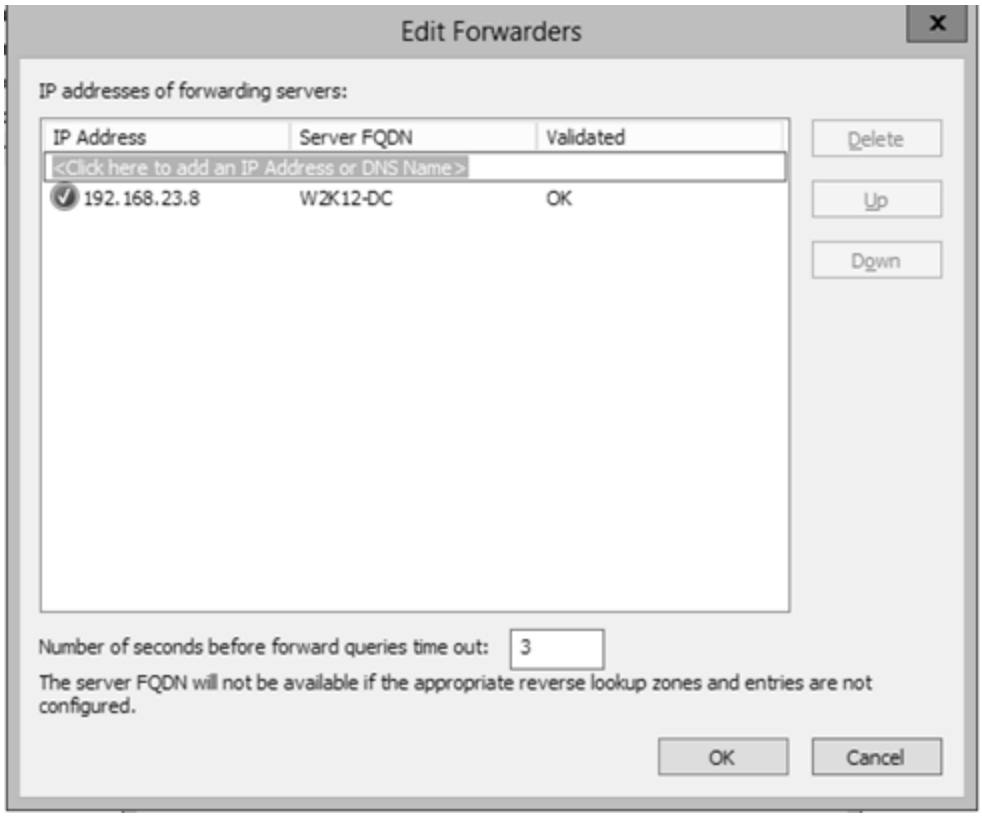
Następnie trzeba się zalogować do serwera DNS domeny innego serwera i przejść do DNS Console (w naszym przypadku jest to W2K12-DFDC.LAB.COM). Dalej należy klinkąć prawym przyciskiem myszy Forwarders, a później properties.



Na zakładce Forwarders należy kliknąć Edit.



Teraz trzeba wpisać adres IP innej domeny DNS (w naszym przypadku jest to W2K12-DC.TEST.COM), a następnie nacisnąć Enter i kliknąć OK.

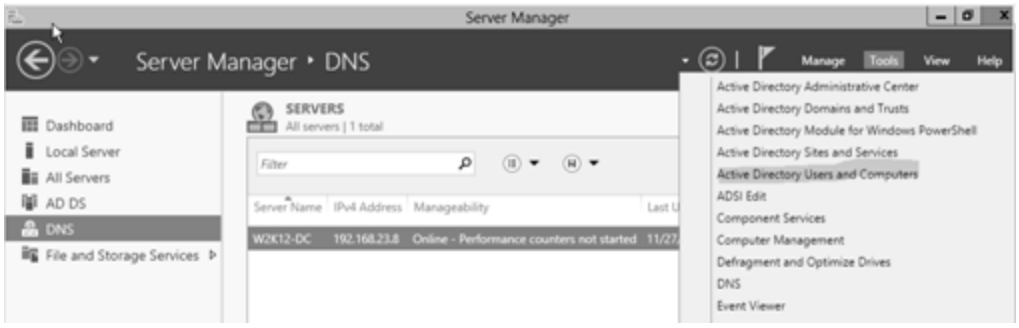


Dalej należy kliknąć Apply i OK.

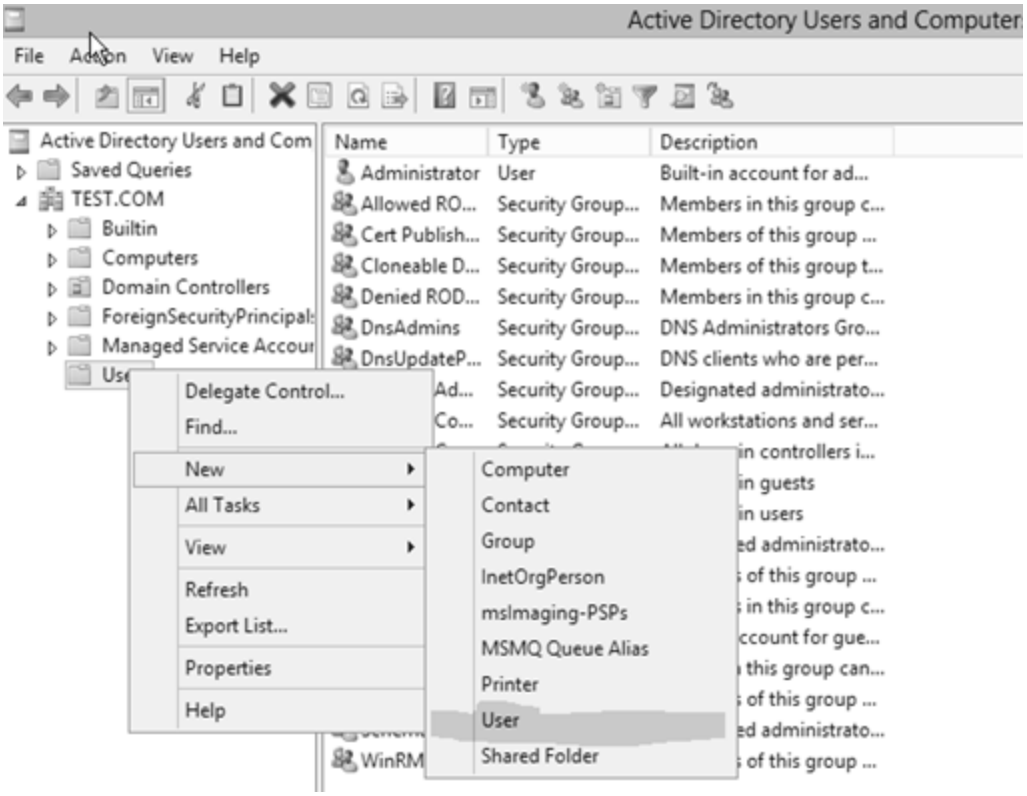
Teraz trzeba utworzyć użytkownika w obu domenach i nadać uprawnienia administratora przedsiębiorstwa, aby utworzyć zaufanie poziomu lasu.

Te same kroki można śledzić na obu DC.

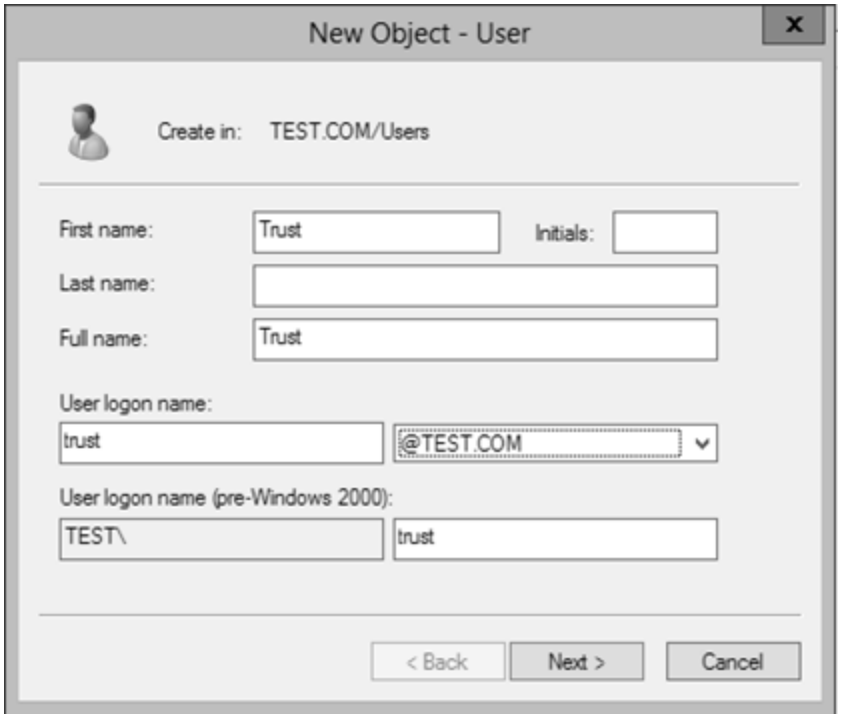
Następnie należy przejść do Active Directory Users and Computers.



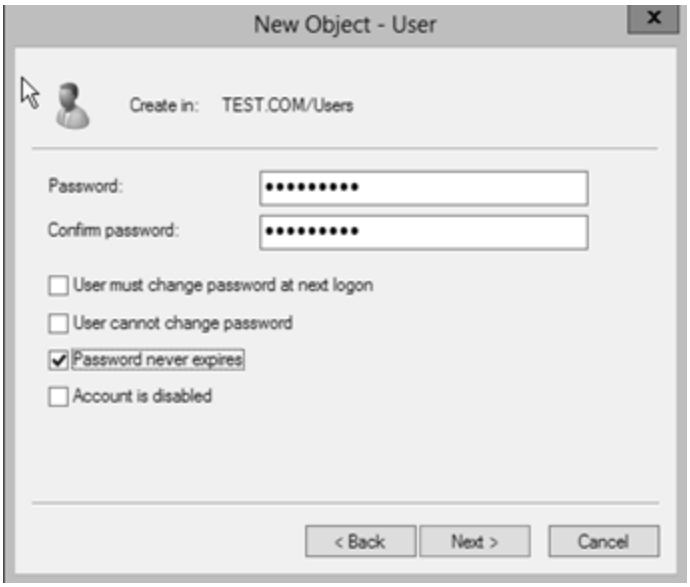
Dalej należy kliknąć prawym przyciskiem myszy Users -> Click New -> Click on User.



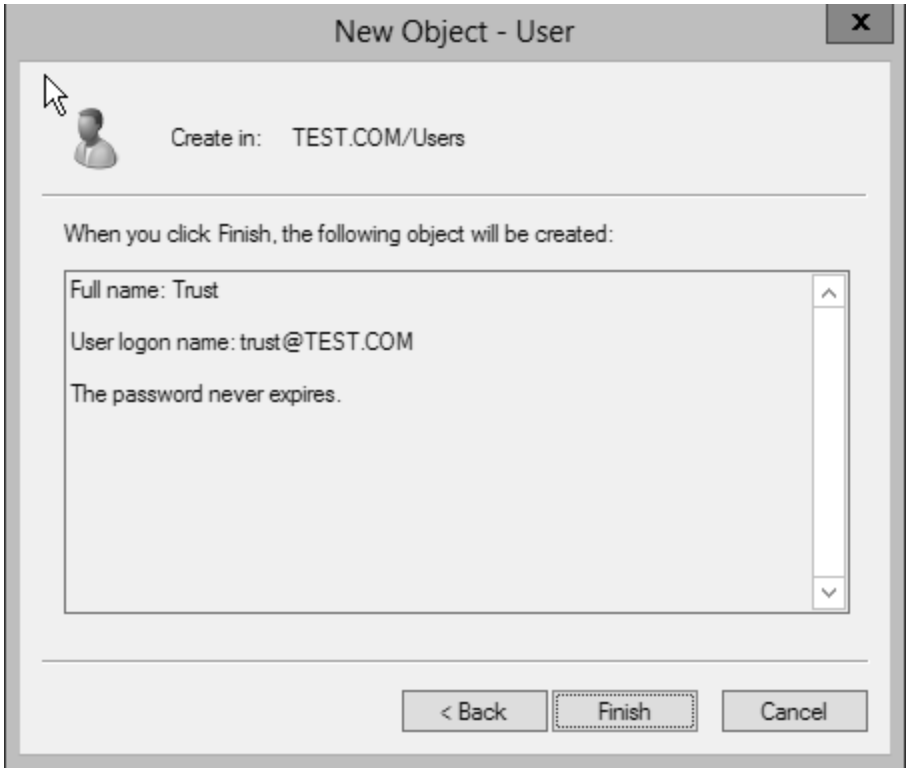
Teraz należy podać szczegóły i kliknąć Next.



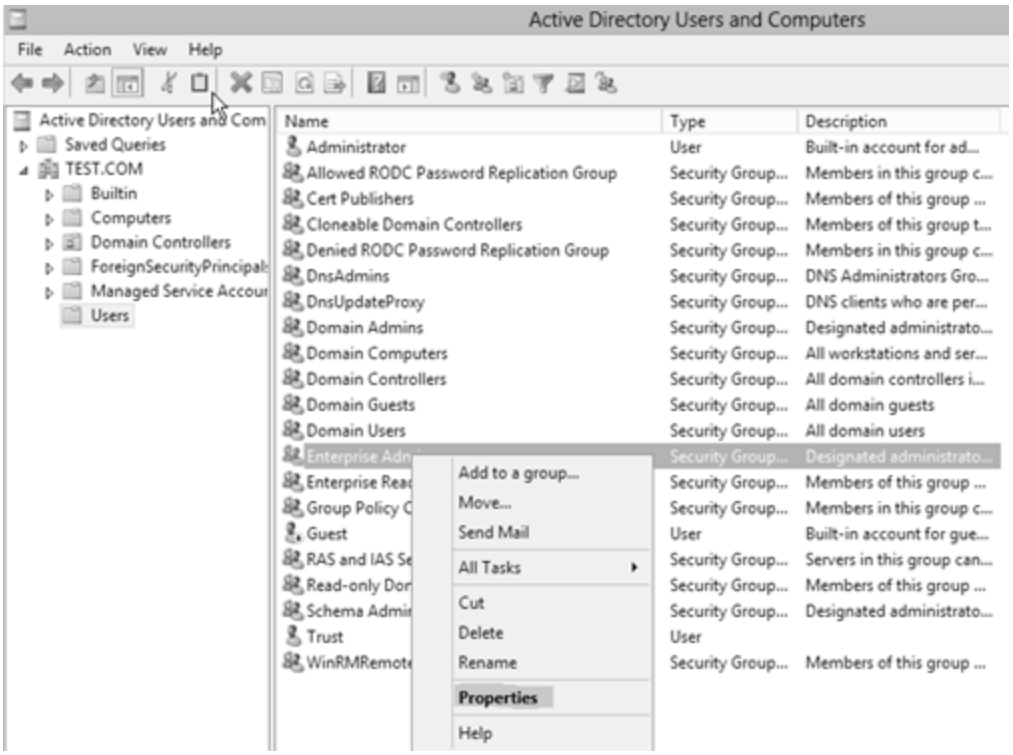
Dalej należy podać hasło i kliknąć Next.



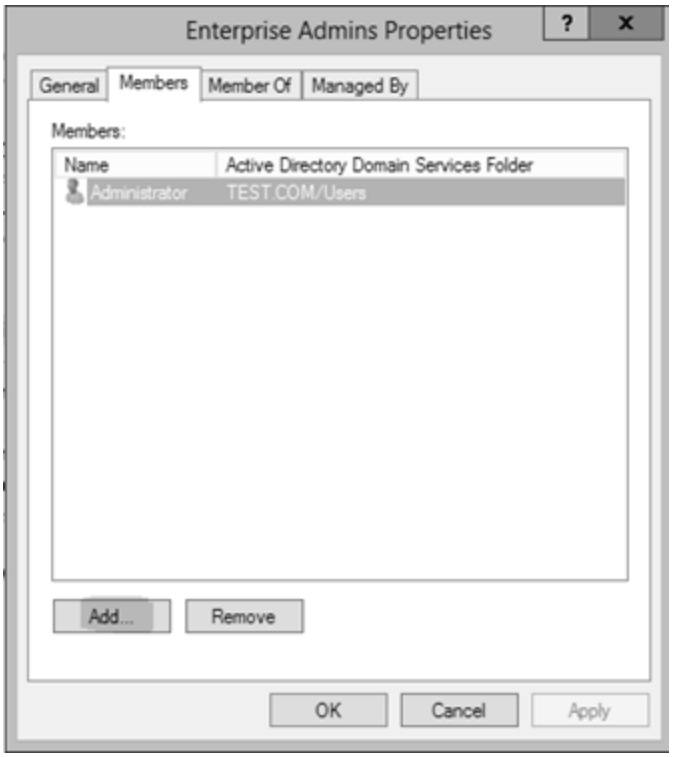
Następnie można już kliknąć Finish.



Następnie prawym przyciskiem myszy należy kliknąć Enterprise Admins group i dalej properties.

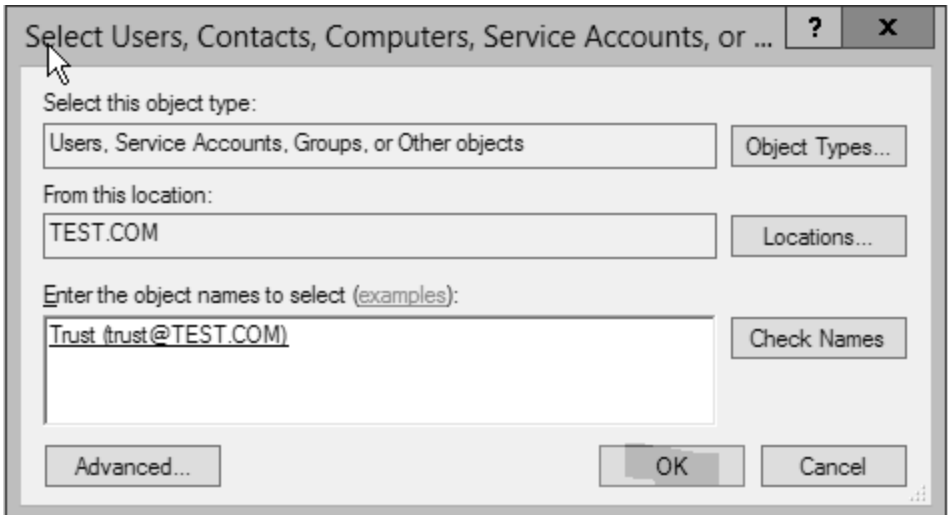


Dalej należy przejść do Members Tab i kliknąć Add.



W następnym oknie należy wpisać nazwę użytkownika i kliknąć Check Names.

Aby przejść dalej, należy kliknąć OK.

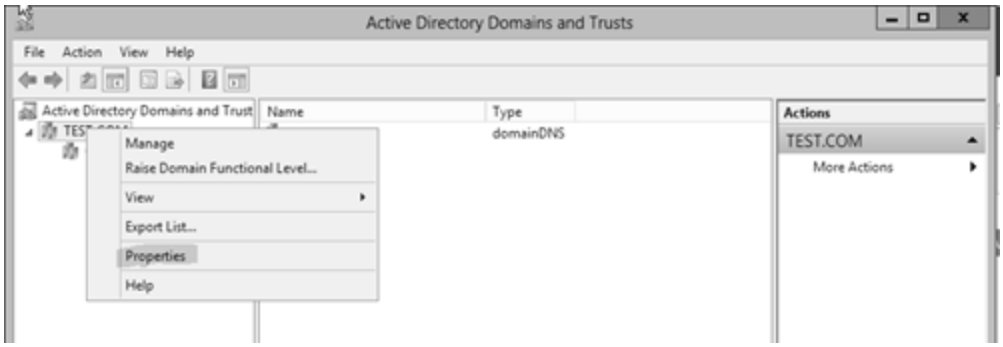


Te same kroki należy wykonać w innej domenie, aby utworzyć użytkownika.

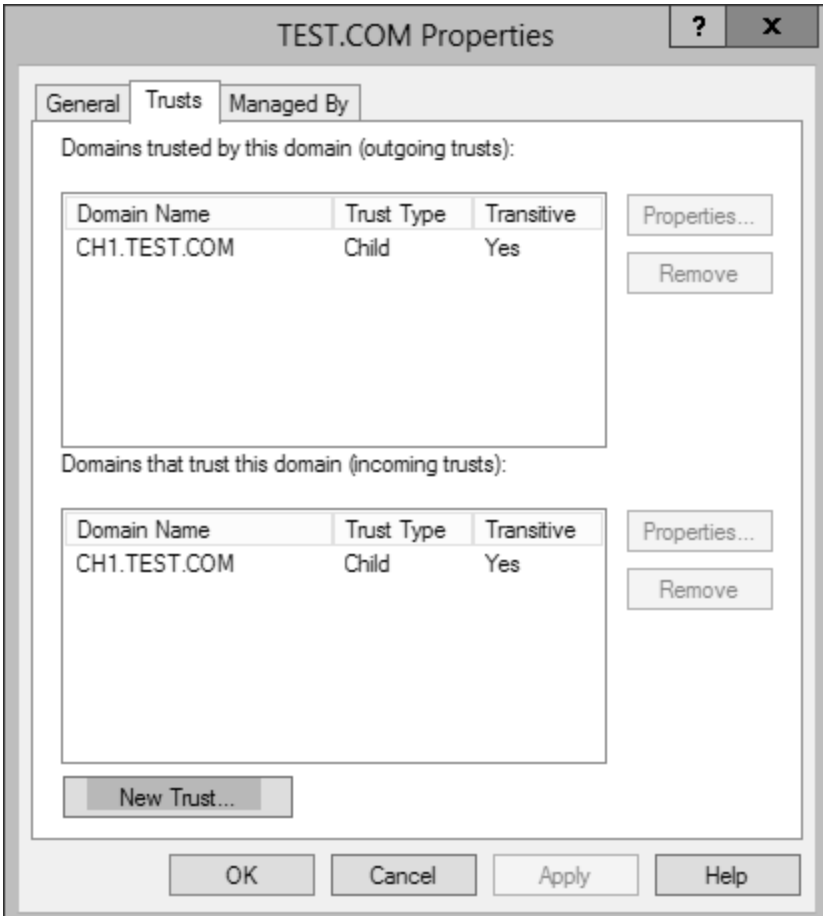
46.1. Tworzenie TRUST

Należy przejść do Active Directory Domains and Trusts.

Dalej należy kliknąć prawym przyciskiem myszy domenę TEST.COM i kliknąć Properties.

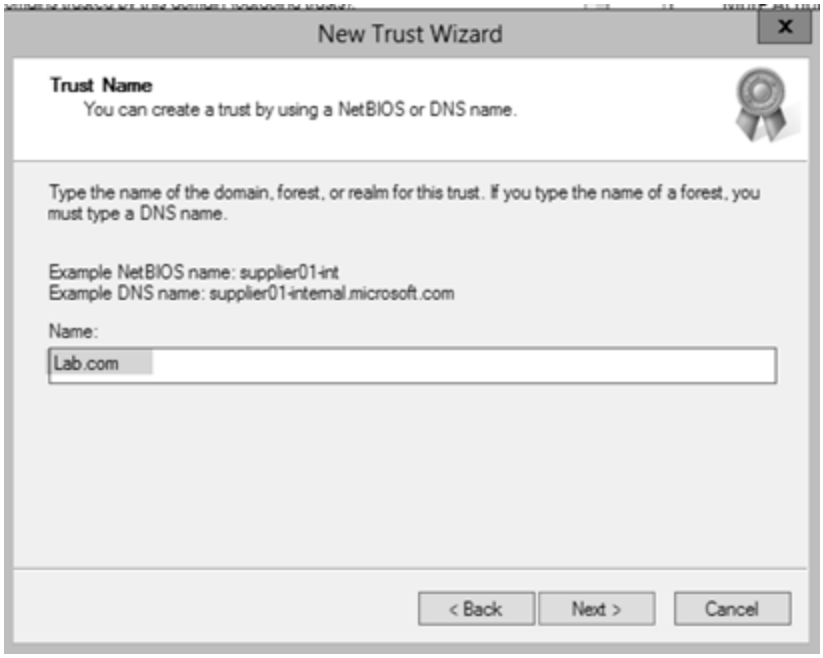


Następnie należy przejść do zakładki Trusts i kliknąć na New Trust.

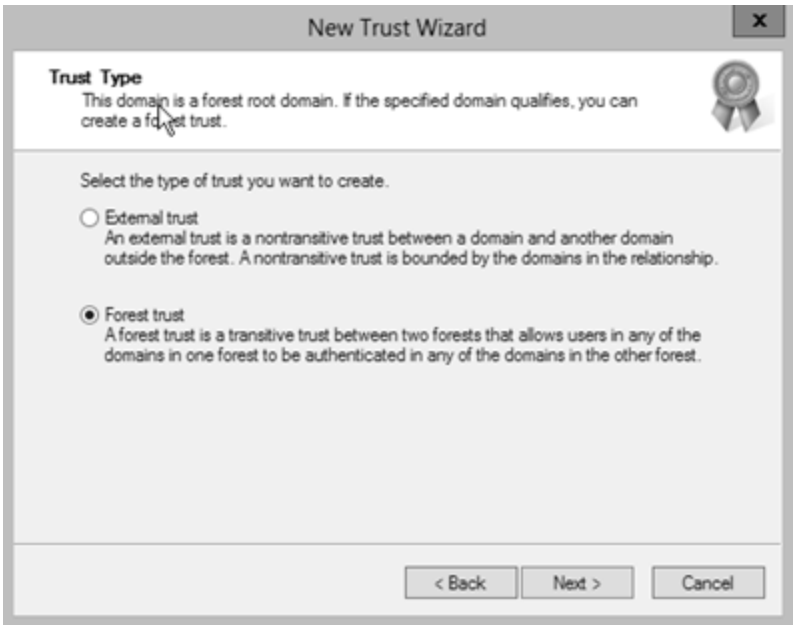


Należy kliknąć Next.

W kolejnym oknie należy wpisać inną nazwę domeny, dla której wymagane jest Trust i kliknąć Next.



Teraz należy wybrać Forest Trust i znów kliknąć Next.

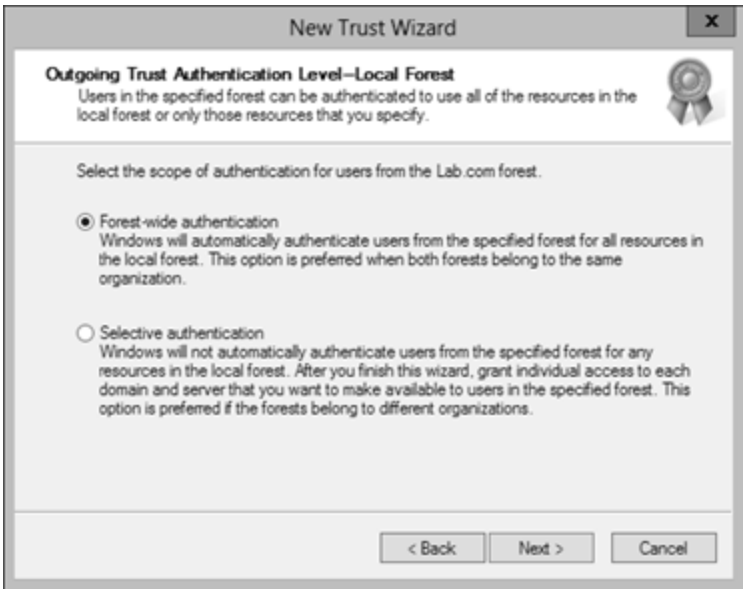


Dalej należy wybrać Two-Way i kliknąć Next.

Następnie należy wybrać Both Sides i kliknąć Next.

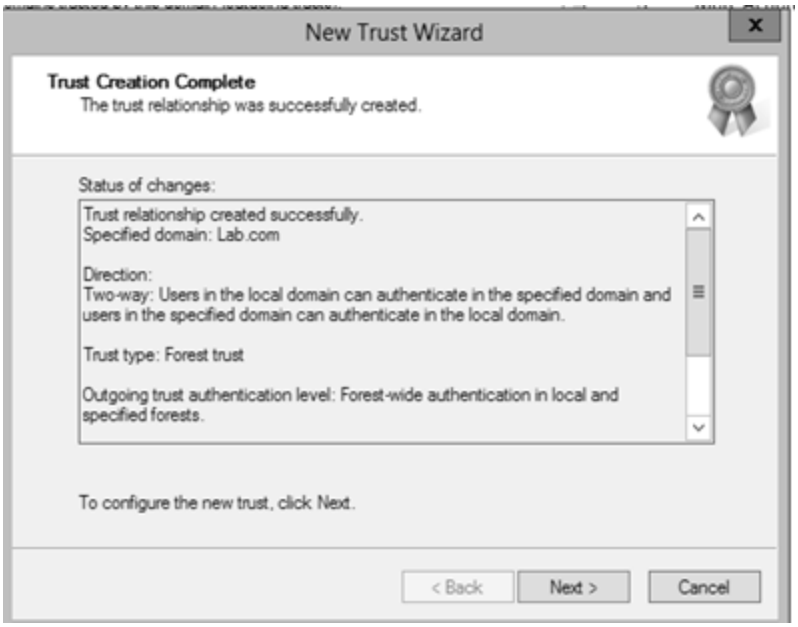
W następnym oknie należy wpisać nazwę użytkownika i kliknąć Next.

Teraz należy wybrać Authentication level i kliknąć Next.

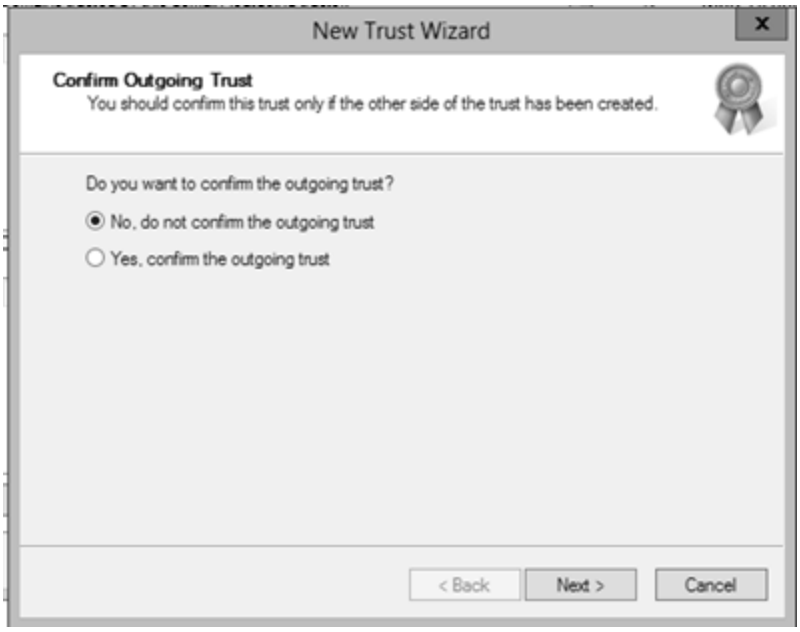


Następnie należy kliknąć Next.

I ponownie należy kliknąć Next.

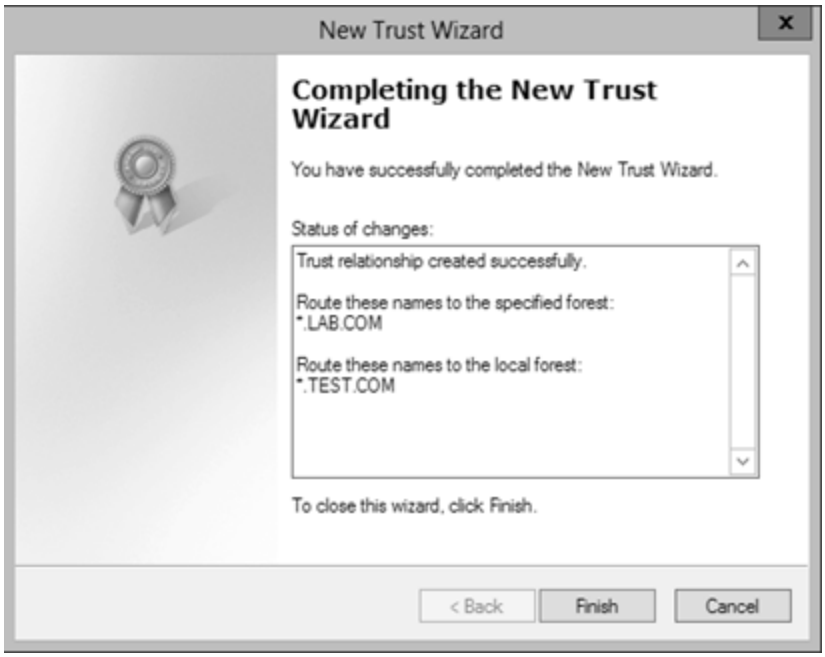


Ponieważ nie mamy jeszcze stworzonych innych Trust, należy kliknąć No i Next.

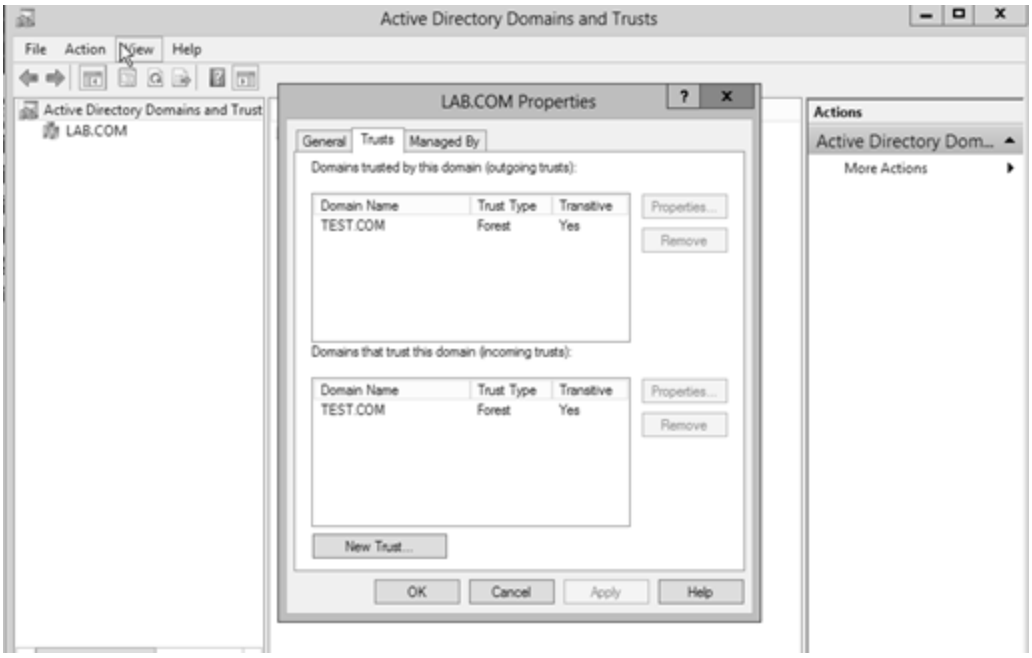


I raz jeszcze należy kliknąć No i Next.

Teraz można już kliknąć Finish.



Jeżeli przejdziemy do Active Directory Domains and Trusts na innej domenie, to będzie można zauważyć TEST.COM trust.



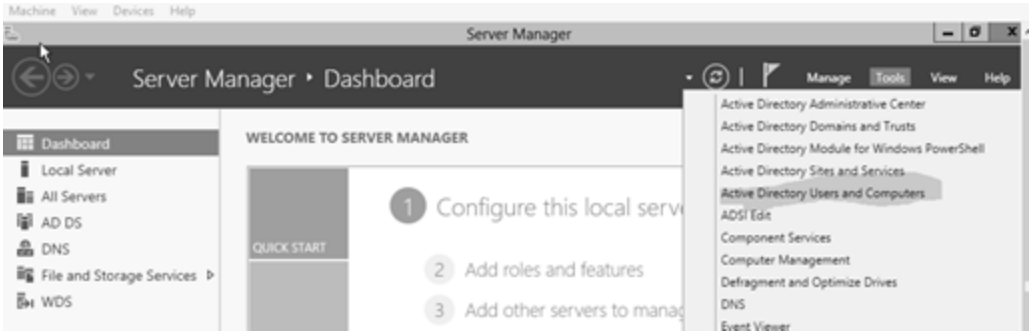
47. Kontroler domeny tylko do odczytu (RODC)

Kontroler RODC jest dodatkowym kontrolerem domeny dla domeny obsługującej tylko do odczytu partycji bazy danych Active Directory. Kontroler RODC jest przeznaczony przede wszystkim do wdrożenia w środowisku oddziału firmy. Oddziały mają zazwyczaj niewielu użytkowników, słabe fizyczne bezpieczeństwo, stosunkowo słabą przepustowość sieci do strony centralnej i małą lokalną wiedzę informatyczną.

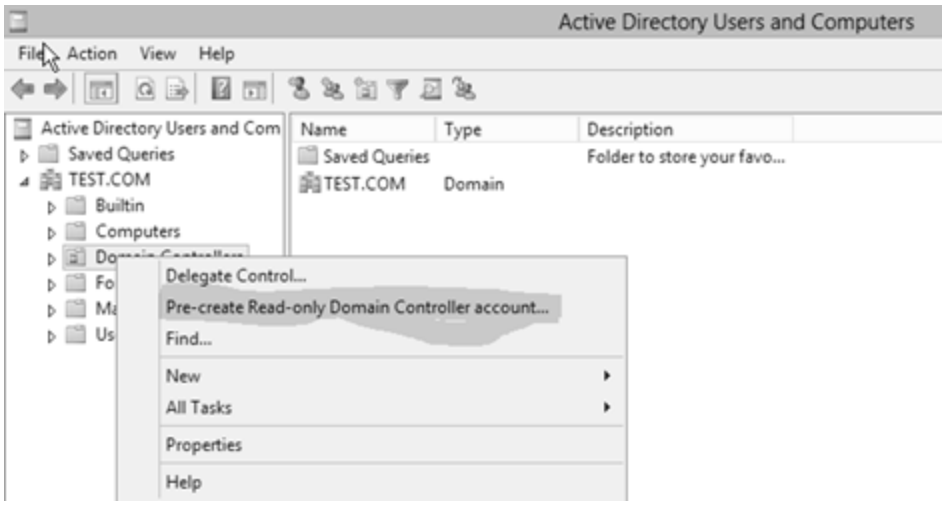
Zanim zaczniemy konfigurować RODC, należy upewnić się, że mamy „Pre-create Read-only Domain Controller

Account”.

Następnie należy zalogować się do Primary Domain Controller i przejść do Active Directory Users and Computers.

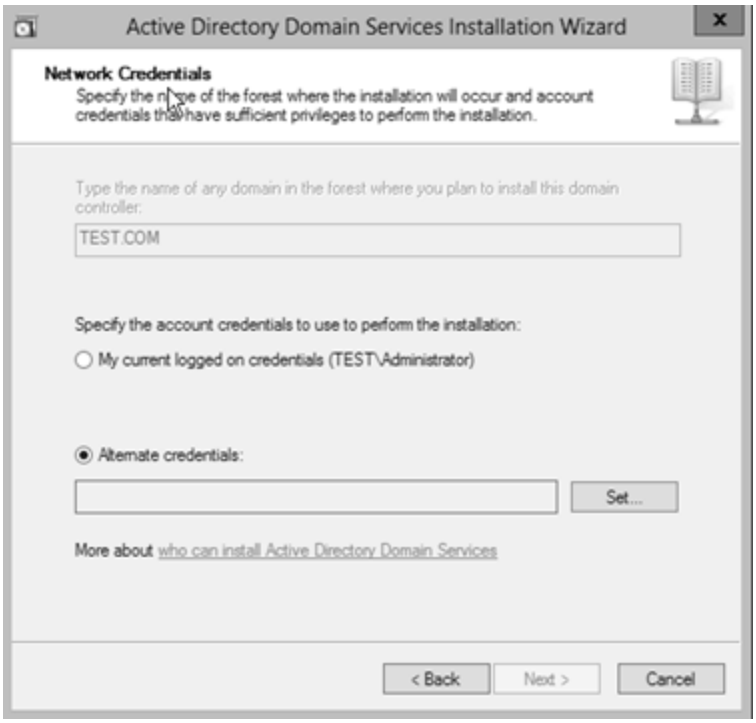


Dalej należy kliknąć prawym przyciskiem myszy Domain Controllers i kliknąć Pre-create Read-only Domain Controller Account.

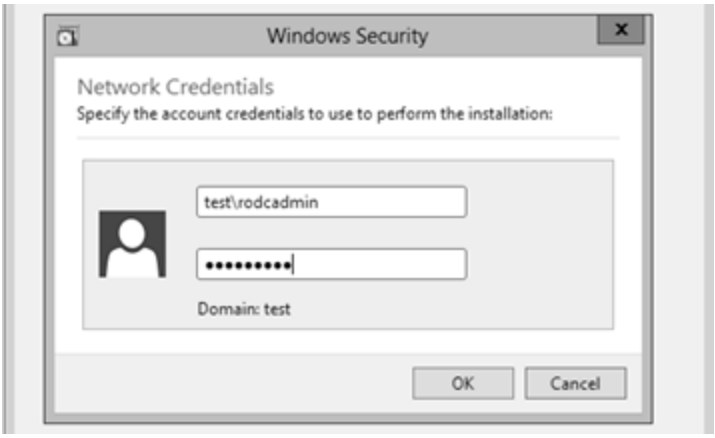


Trzeba kliknąć Next w kreatorze.

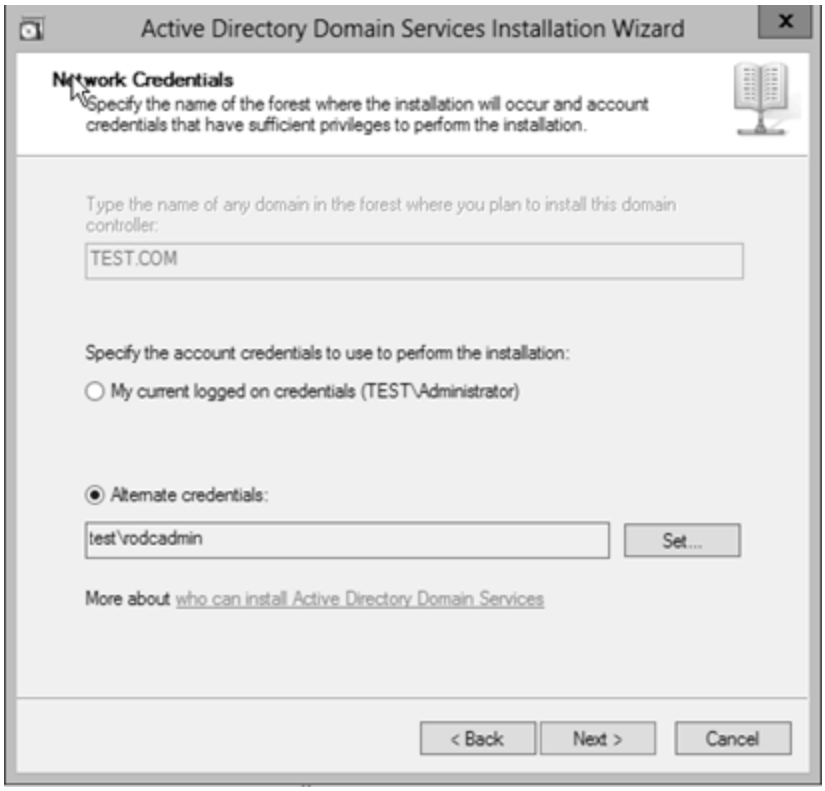
Następnie należy kliknąć alternate credentials. Można również użyć zalogowanego użytkownika. Stworzyłem osobnego użytkownika, więc ustawię właśnie tego.



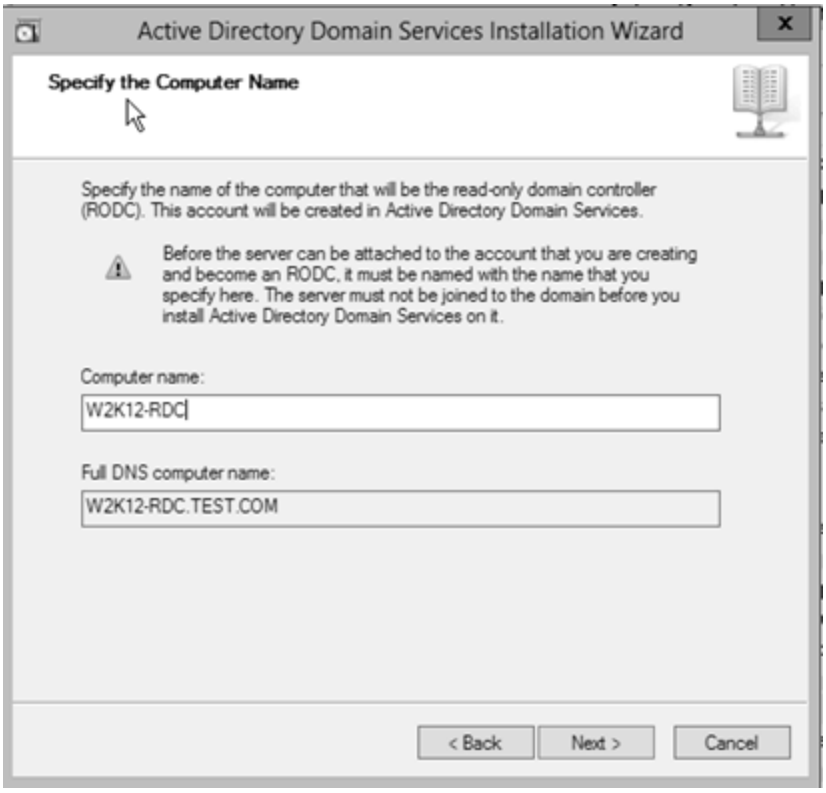
Należy wpisać dane i kliknąć OK.



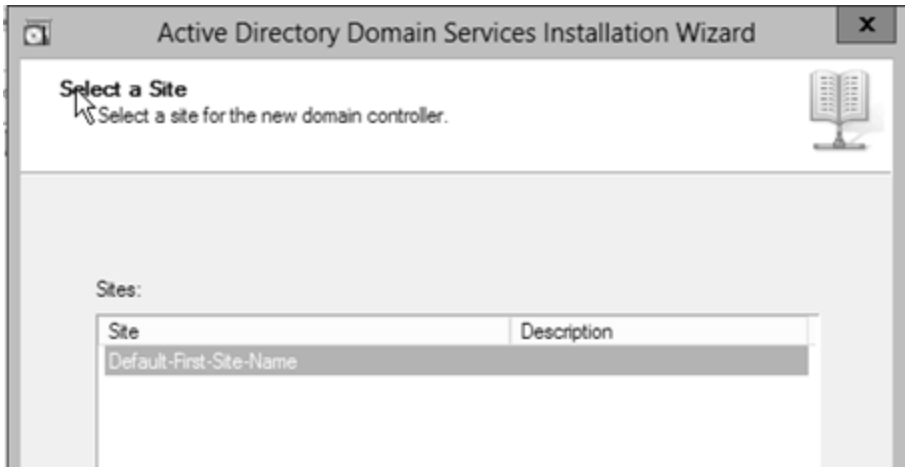
Teraz należy kliknąć Next.



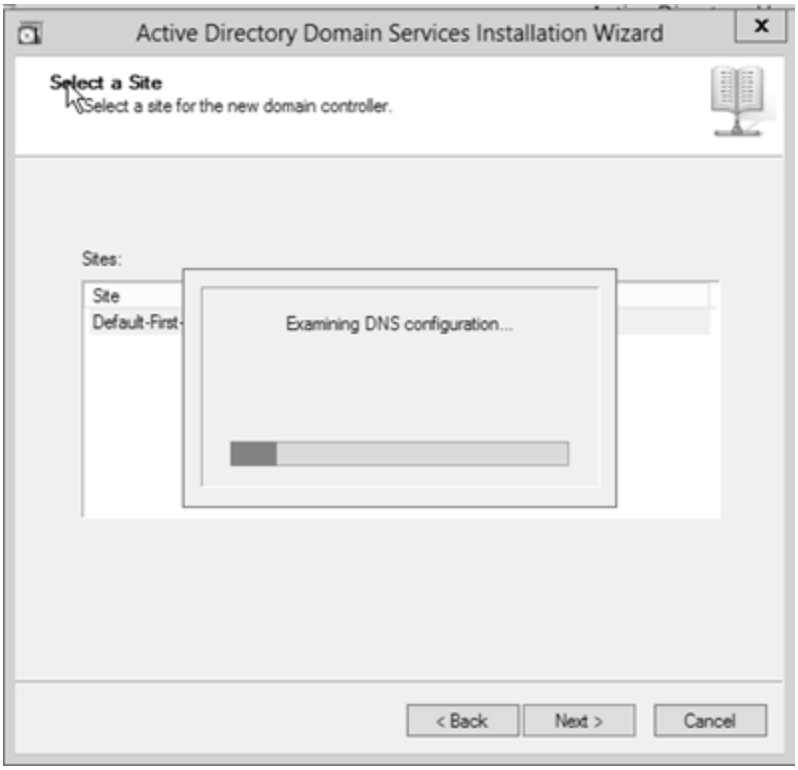
Następnie należy wpisać nazwę serwera, do którego chcemy utworzyć RDC.



Zanim przejdziemy dalej, należy wybrać Site.

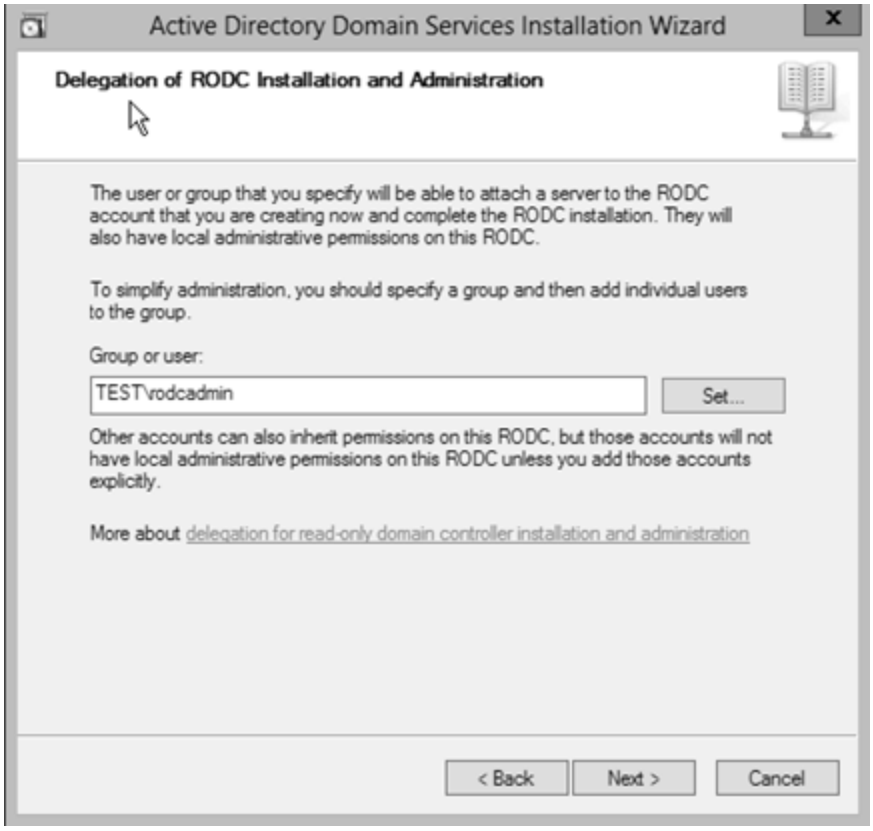


Następnie należy kliknąć Next.

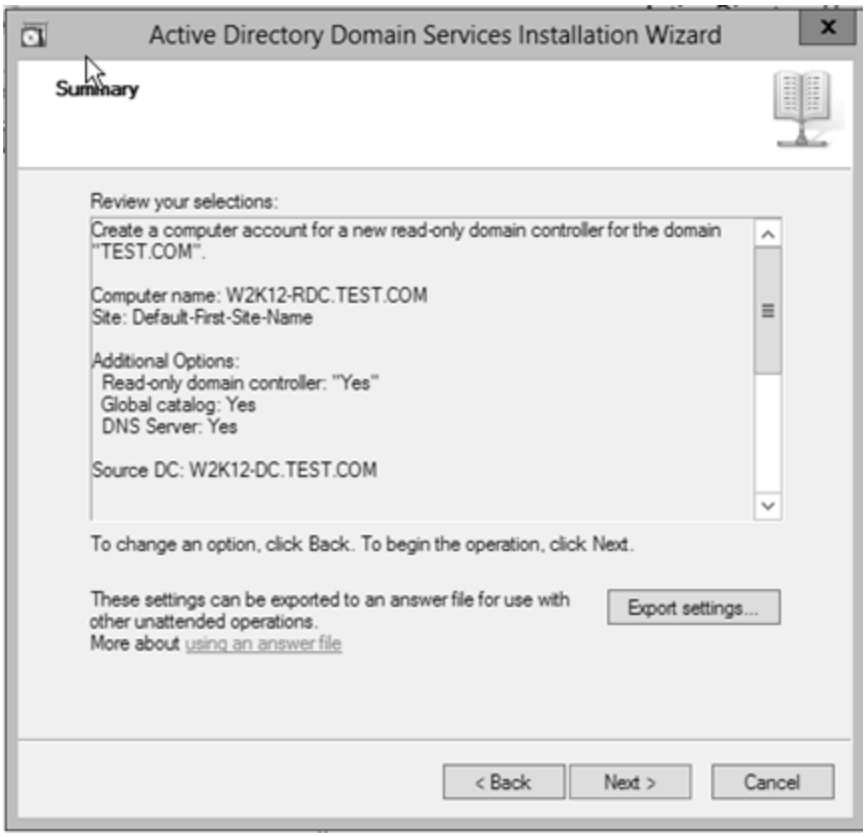


Dalej należy wybrać dodatkowe opcje i ponownie kliknąć Next.

Następnie należy podać User lub Group i kliknąć Next. Dla celów demonstracyjnych utworzyłem użytkownika, jednak utworzyć utworzyć grupę, dzięki czemu będzie można jej używać w dowolnym momencie.

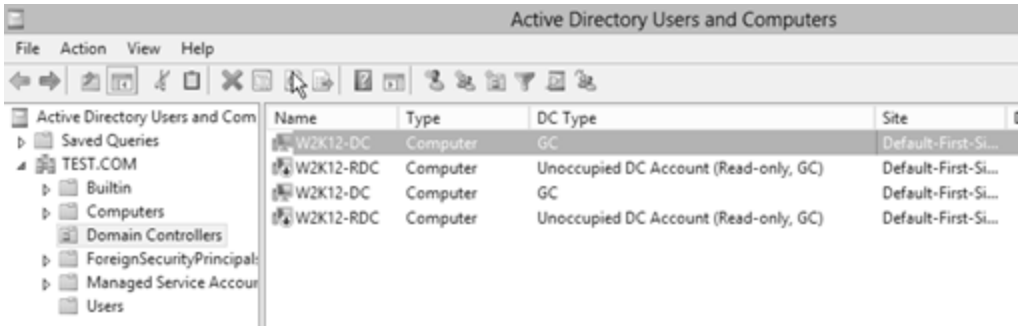


Dalej należy kliknąć Next.



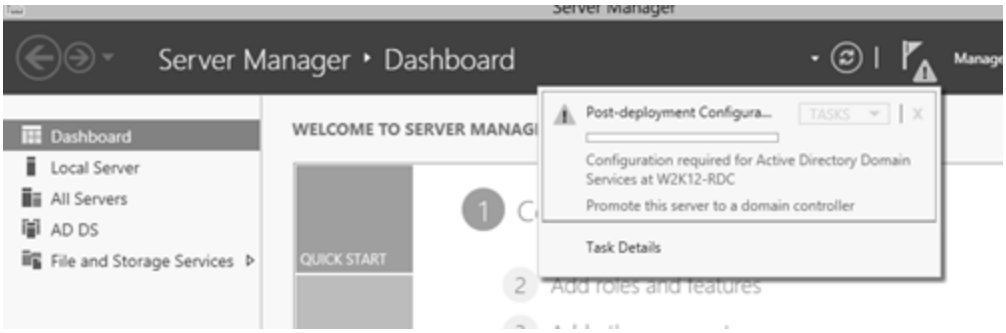
Aby zakończyć, należy kliknąć Finish.

Mamy teraz utowrzone swoje konto RODC i wymienione poniżej pod kontrolerami domeny.

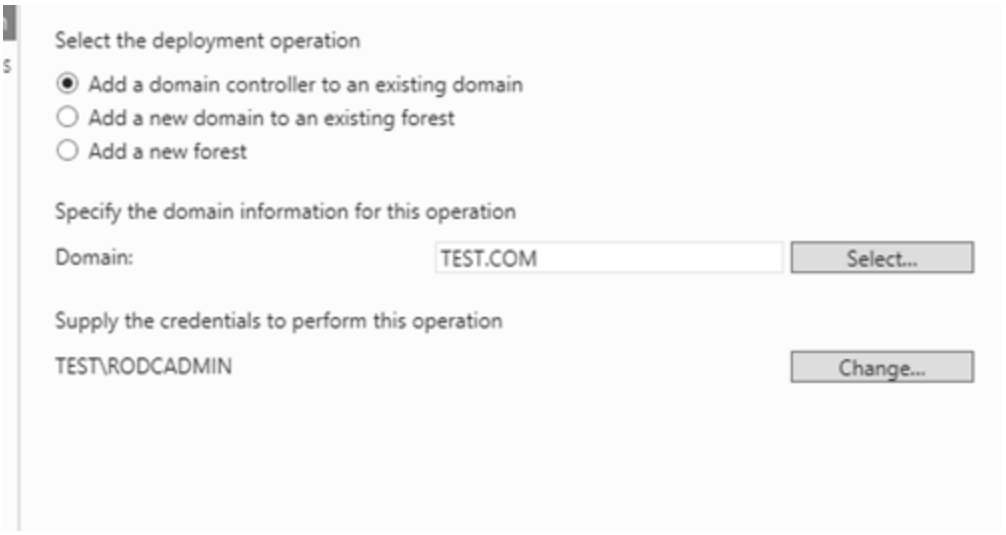


Trzeba się zalogować do serwera, który chcemy skonfigurować jako RDC, a następnie zainstalować role AD.

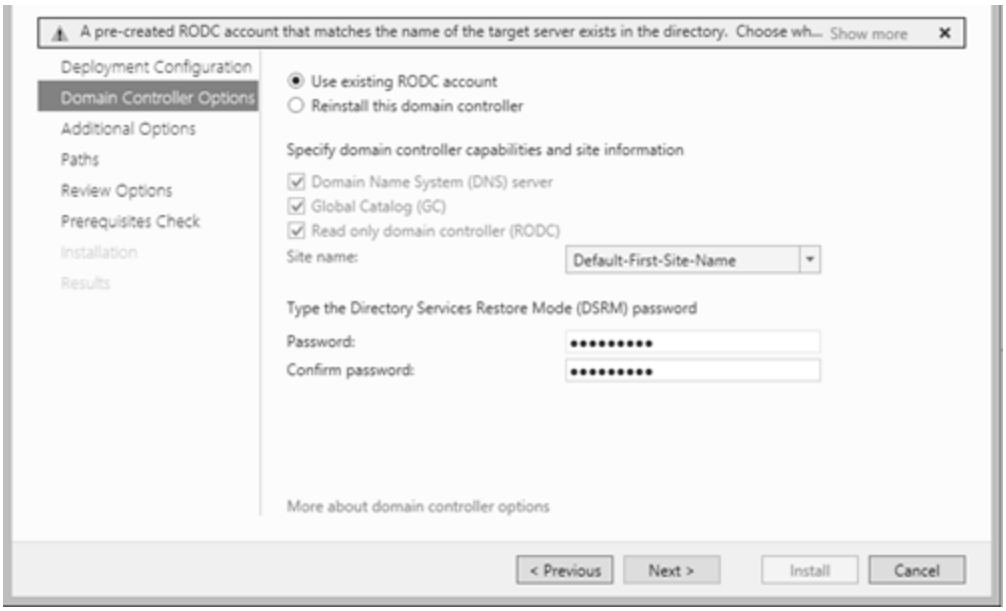
Po zainstalowaniu AD role należy przejść do server Manager Dashboard i kliknąć promote this server as domain Controller.



Następnie należy wybrać Add Domain controller to existing domain i wybrać domenę. W razie potrzeby należy podać dane.



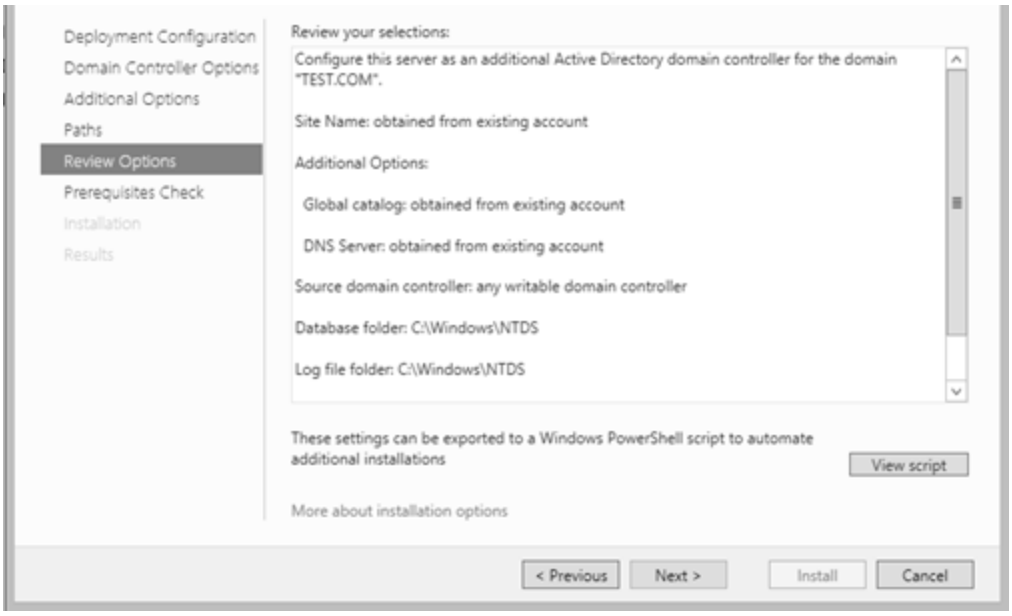
Dalej trzeba wybrać Use existing RODC account, następnie site, podać hasło DSRM i kliknąć Next.



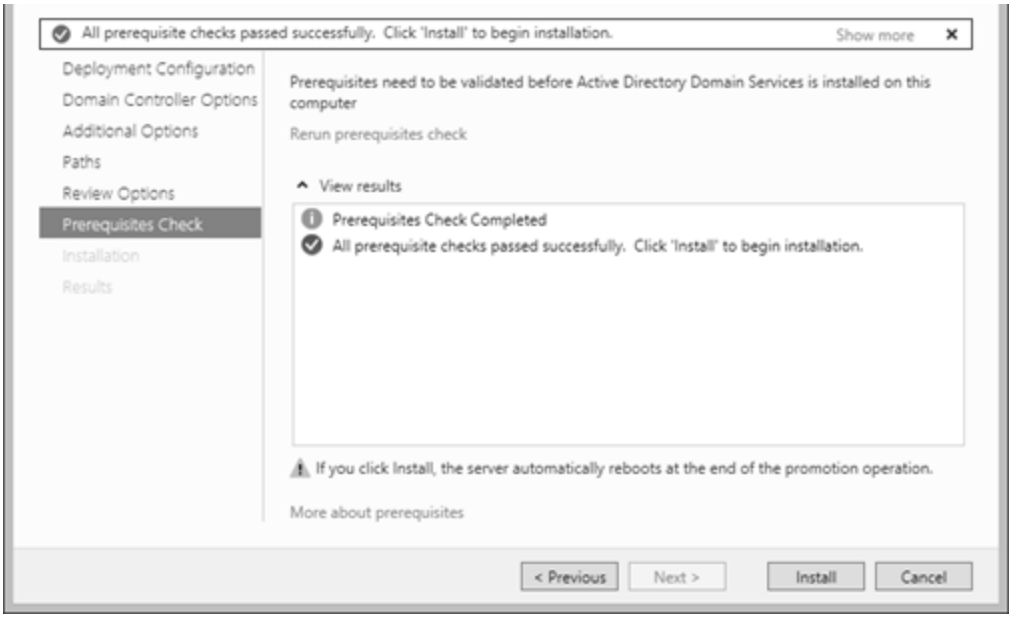
Teraz należy wybrać replikę DC, który jest głównym kontrolerem domeny i kliknąć Next.

Następnie trzeba wybrać lokalizację folderu database, log files i SYSVOL i kliknąć.

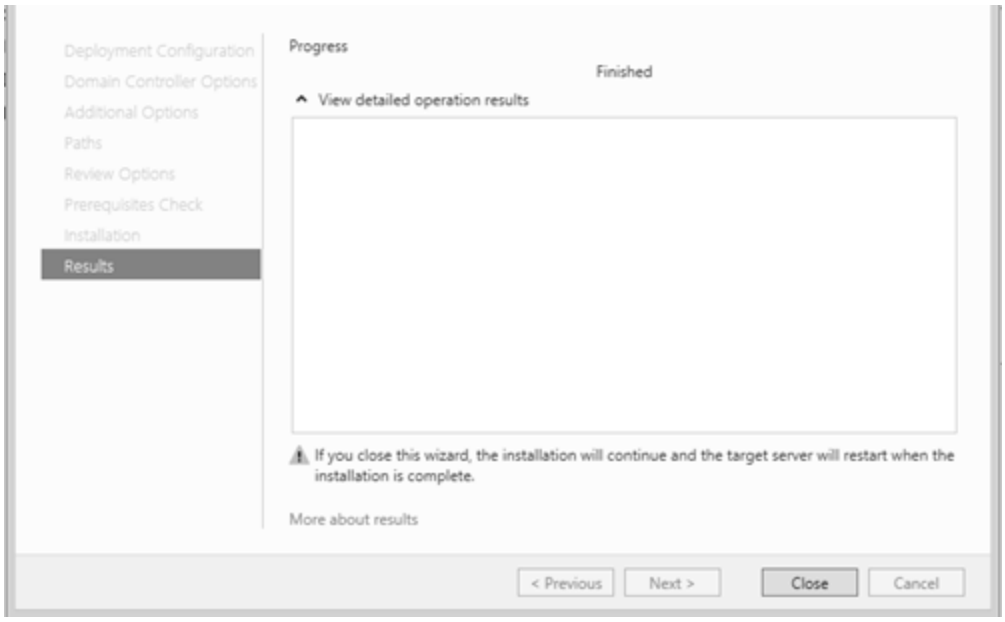
Dalej należy kliknąć Next.



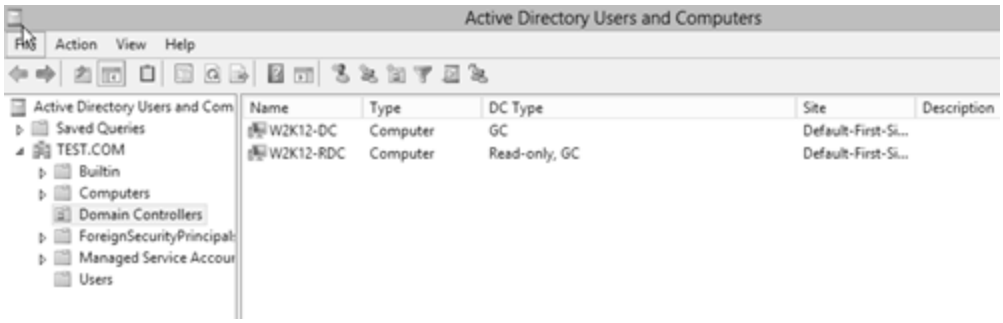
A gdy zostaną spełnione wszystkie wymagania wstępne, można już kliknąć Install.



Po zakończeniu instalacji należy kliknąć Finish i Serwer uruchomi się ponownie automatycznie.

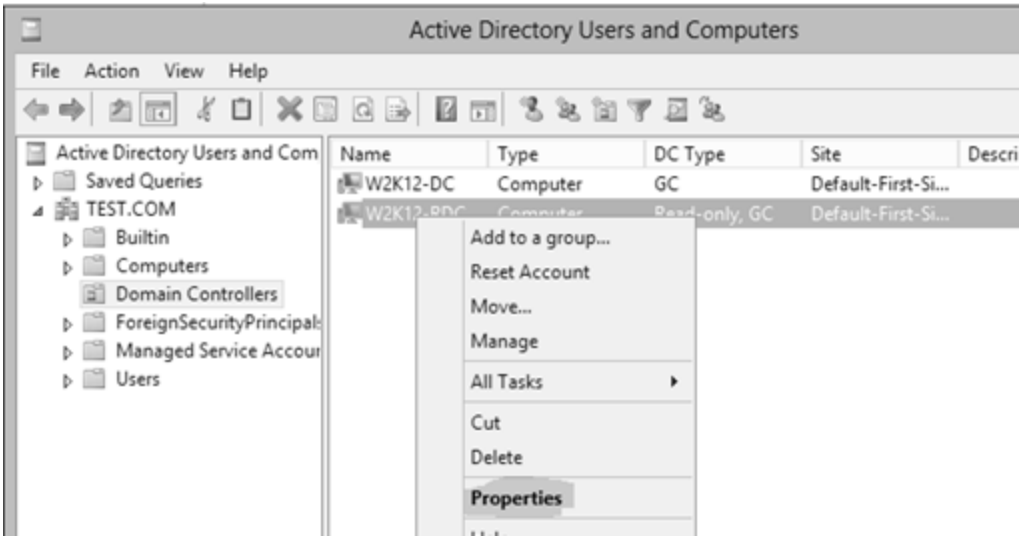


Po ponownym uruchomieniu serwera kontroler Read Only Domain będzie gotowy.

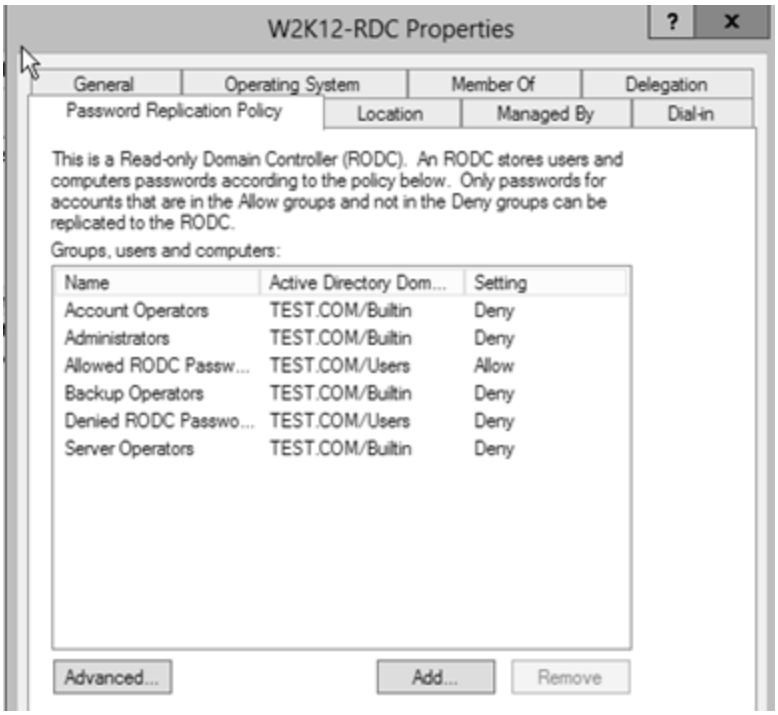


Po skonfigurowaniu kontrolera RODC należy przejść do Active Directory Users and Computers.

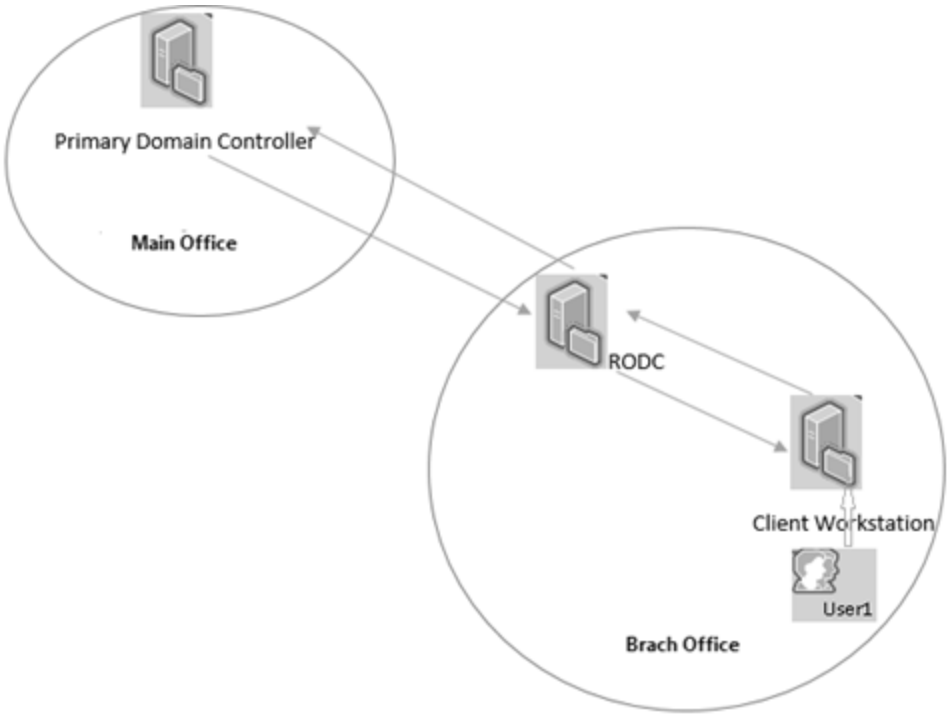
Dalej trzeba kliknąć prawym przyciskiem myszy RODC, a następnieproperties.



Następnie należy przejść do zakładki Password Replication Policy, i skonfigurować replikację haseł, która powinna być dozwolona za pośrednictwem usługi RDC, a następnie kliknąć przycisk OK.



48. Jak działa uwierzytelnianie użytkownika.



Biuro oddziału zawiera kontroler domeny RODC, a główny kontroler domeny znajduje się w biurze głównym. Użytkownik user1 próbuje zalogować się do swojego komputera w oddziale. Następuje sekwencja.

1. Stacja robocza klienta przygotowuje żądanie uwierzytelnienia Kerberos i wysyła je do RODC.

2. RODC otrzymuje żądanie uwierzytelnienia Kerberos z komputera klienckiego. Kontroler RODC sprawdza lokalną bazę danych, aby sprawdzić, czy hasło jest buforowane dla stacji roboczej klienta. Ponieważ nie jest buforowany, RODC nie może uwierzytelnić stacji roboczej klienta.

3. RODC przekazuje żądanie uwierzytelnienia Kerberos ze stacji roboczej klienta do zapisywalnego kontrolera domeny w głównym biurze, który jest głównym kontrolerem domeny w naszym przypadku.

4. Główny kontroler domeny odbiera żądanie uwierzytelnienia Kerberos i jest w stanie uwierzytelnić stację roboczą klienta za pomocą pełnej kopii bazy danych Active Directory.

5. Główny kontroler domeny generuje odpowiedź żądania uwierzytelnienia Kerberos dla stacji roboczej klienta i wysyła ją do kontrolera RODC.

6. Kontroler RODC wykonuje następujące dwa zadania:

a. żąda od podstawowego kontrolera domeny replikowania referencji dla stacji roboczej klienta do repliki bazy danych Active Directory,

b. przesyła dalej odpowiedź na żądanie uwierzytelniania Kerberos do stacji roboczej klienta.

7. Główny kontroler domeny sprawdza zasady replikacji haseł, że stacja robocza klienta może buforować hasło do konta za pomocą kontrolera RODC.

8. Poświadczenia stacji roboczej klienta są replikowane z podstawowego kontrolera domeny do kontrolera RODC, a stacja robocza klienta jest dodawana do listy „Kont, których hasła są przechowywane na tym kontrolerze domeny tylko do odczytu” kontrolera RODC.

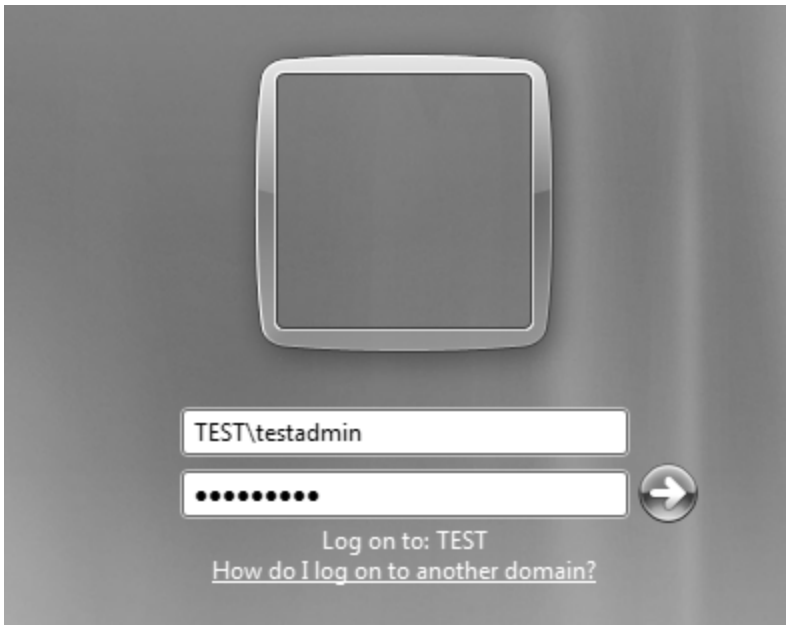
9. RODC buforuje hasło do konta dla stacji roboczej klienta.

Sprawdzanie przykładu procesu logowania

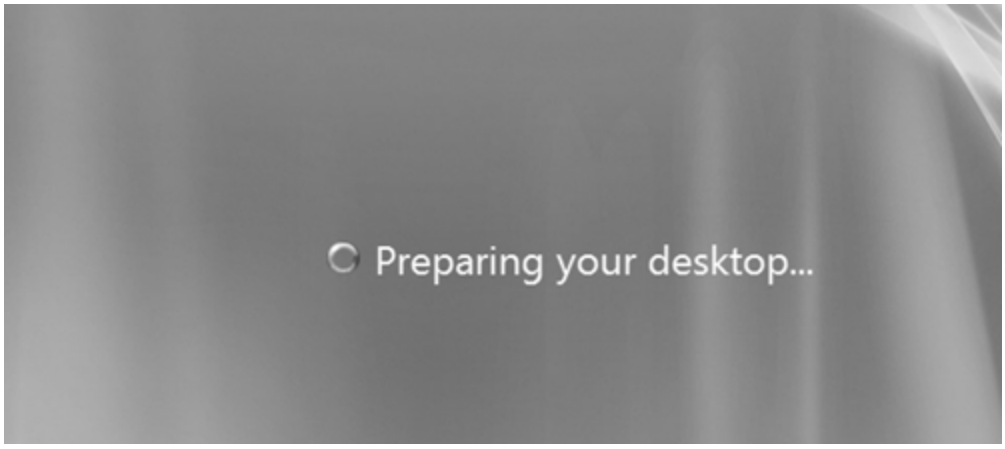
Mamy serwer W2K8 dodany do domeny. Mamy użytkownika testadmin, który jest członkiem domeny administracji. Ustawiono podstawowy kontroler domeny jako niedostępny, a kontroler RODC jest dostępny. Próbujemy zalogować się do serwera W2K8 użytkownikiem testadmin, ale kończy się to błędem.

Wynika to z faktu, że obecnie nasz kontroler RODC nie ma hasła do tego użytkownika w pamięci podręcznej, a zatem nie może uwierzytelnić tego użytkownika w przypadku braku podstawowego kontrolera domeny.

Teraz należy włączyć główny kontroler domeny i zalogować się do serwera na tym samym koncie.



Teraz można zalogować się na serwer.



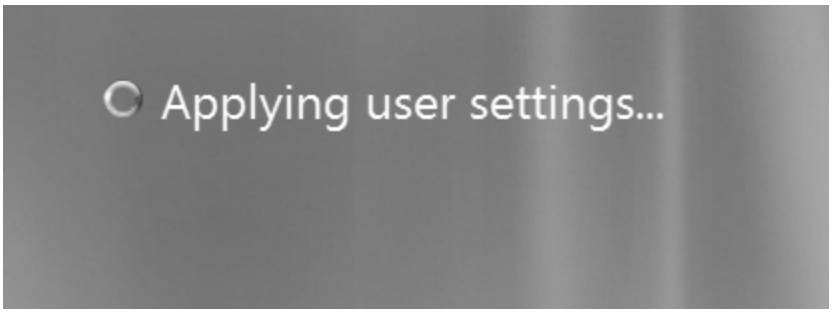
Odkąd mamy nasz główny kontroler domeny, można się bez problemu zalogować.

Ponieważ nasz kontroler RODC nie miał w pamięci podręcznej poświadczeń, przekazał żądanie do podstawowego kontrolera domeny. Główny kontroler domeny sprawdził swoją bazę danych i stwierdził, że może uwierzytelnić użytkownika testadmin. Następnie wyśle odpowiedź uwierzytelniania do kontrolera RODC. RODC przesyła następnie odpowiedź do W2K8 i uwierzytelnia

logowanie użytkownika. RODC poprosi również główny kontroler domeny o replikację referencji przy użyciu bazy danych RODC. Główny kontroler domeny sprawdzi regułę replikacji haseł i sprawdzi, czy może zreplikować poświadczenia za pomocą kontrolera RODC, a następnie zreplikuje poświadczenia. RODC buforuje następnie informacje o referencjach.

Teraz znowu można sprawić, że nasz podstawowy kontroler domeny będzie niedostępny i spróbować zalogować się do W2K8.

Tym razem uda się zalogować nawet podczas nieobecności na głównym kontrolerze domeny.



Ponieważ poświadczenia są buforowane za pomocą kontrolera RODC, uwierzytelnianie będzie działać.

49. Veeam

Veeam zapewnia rozwiązanie do ochrony środowiska wirtualnego. Zapewnia możliwość tworzenia kopii zapasowych i replikacji oraz ułatwia odzyskiwanie / przywracanie dowolnego środowiska wirtualnego lub jego obiektów.

Zapewnia wsparcie dla Hyper-V, VMWARE, Microsoft SNB3, Microsoft Windows i Linux.

Veeam pozwala na:

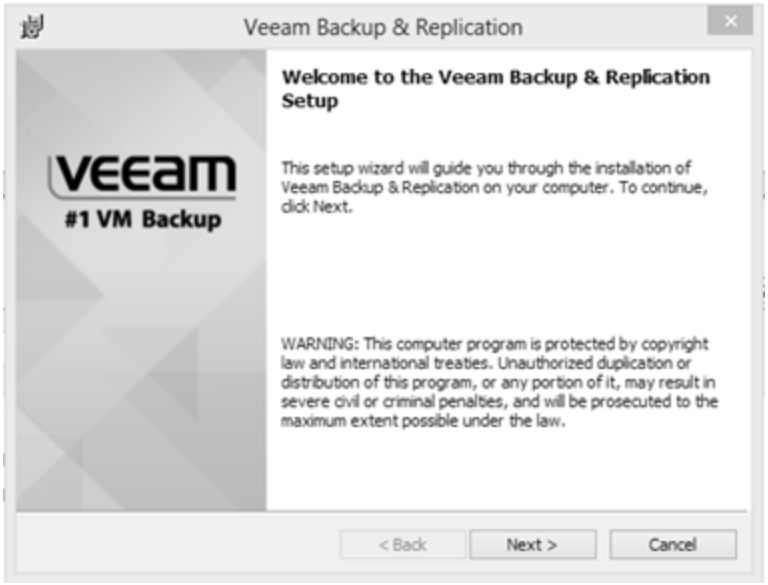
☐ Natychmiastowe odzyskanie uszkodzonej maszyny wirtualnej, zmniejszając w ten sposób przestoje produkowanych maszyn wirtualnych do minimum.

☐ Sprawdzenie możliwość odzyskania każdej kopii zapasowej, uruchamiając i testując maszyny wirtualne bezpośrednio z kopii zapasowych maszyn wirtualnych w odizolowanym środowisku.

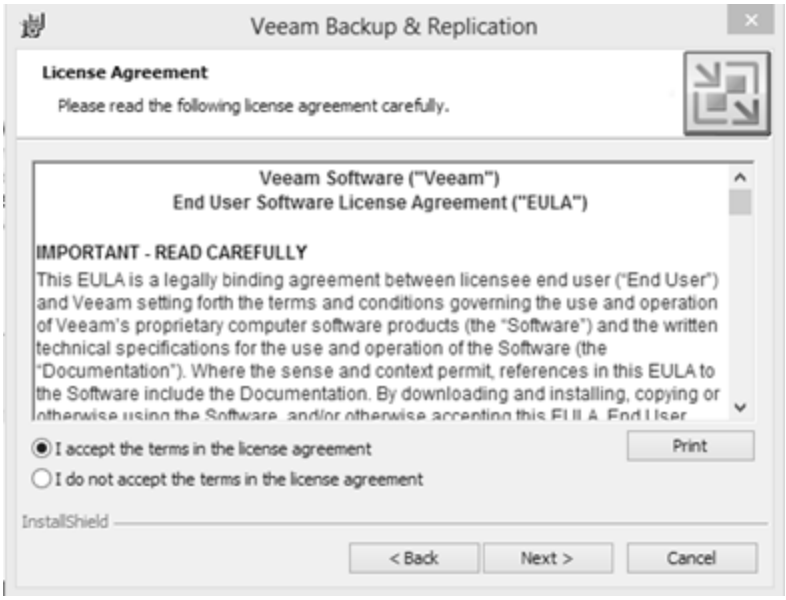
☐ Przywrócenie elementów ze wszystkich zwirtualizowanych aplikacji za pomocą U-AIR.

49.1. Instalacja VEEAM

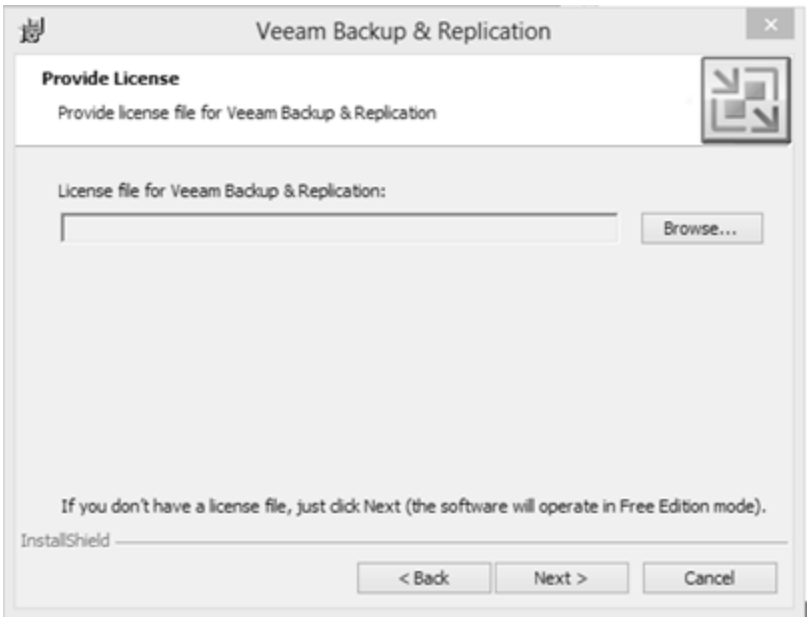
Należy uruchomić kreatora instalacji i kliknąć Next.



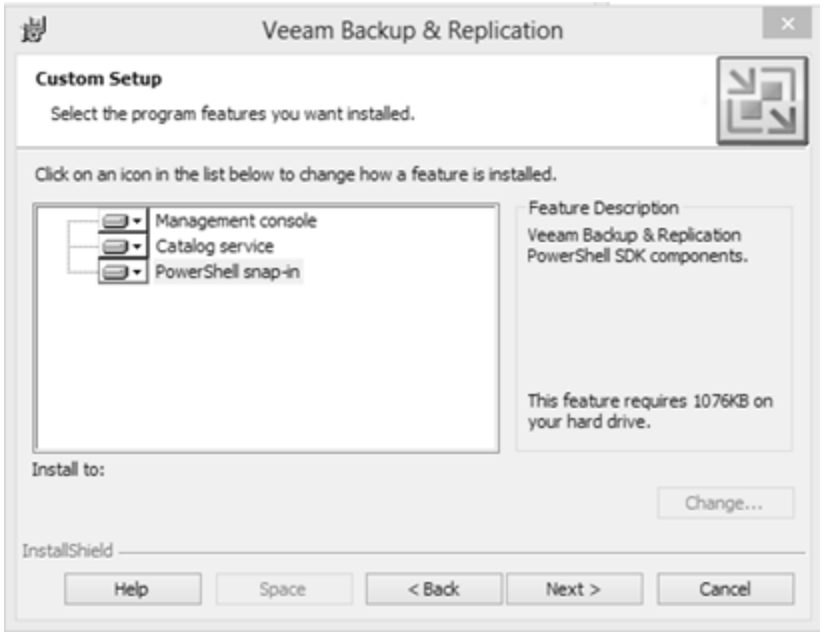
Teraz należy zaakceptować license Agreement i kliknąć Next.



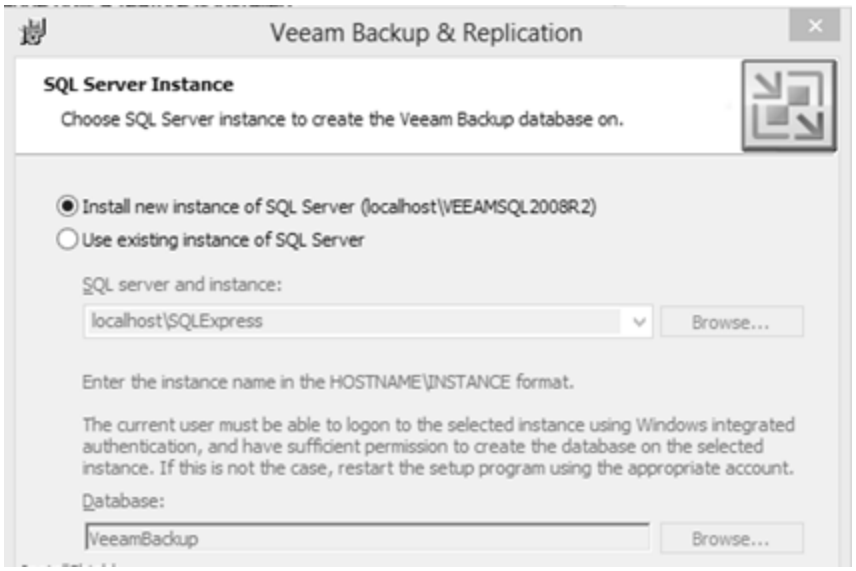
Następnie należy podać License File i ponownie kliknąć Next.



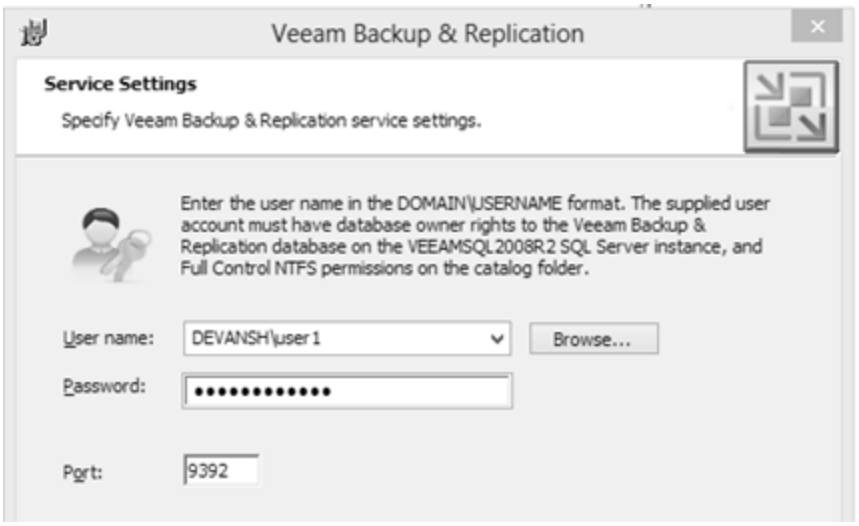
Należy wybrać opcje instalacji i kliknąć Next.



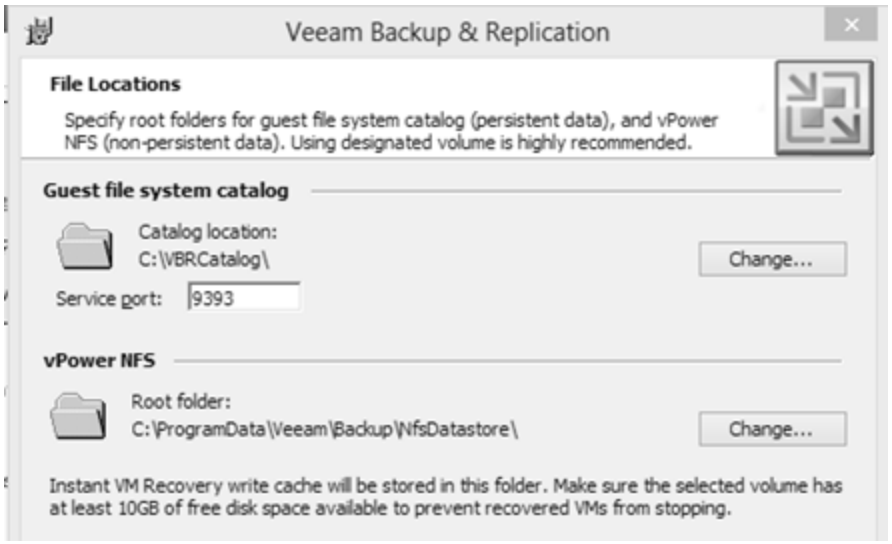
Jeśli już posiadamy ustawienia SQL w swoim środowisku, można utworzyć na nim instancję. Jeśli nie, można wybrać install SQLexpress i utworzyć na nim instancję.



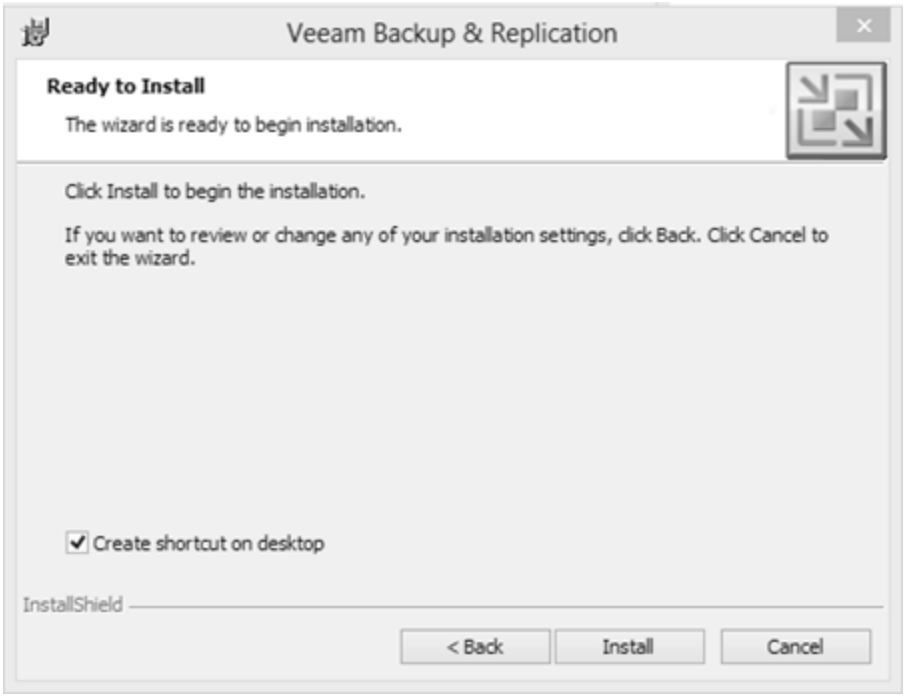
Następnie należy podać dane i kliknąć Next.



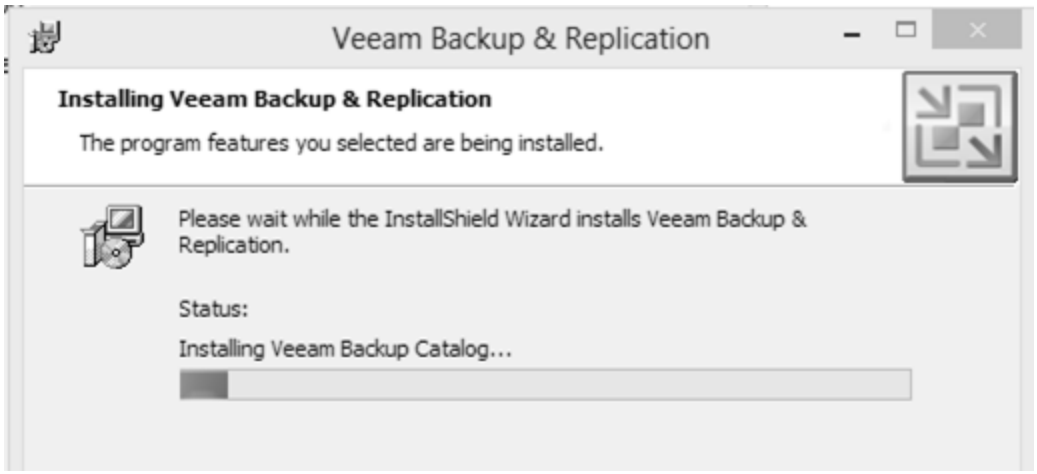
Dalej należy wybrać katalog Lokalizator VPower folder NFS i port serwisowy dla katalogu.

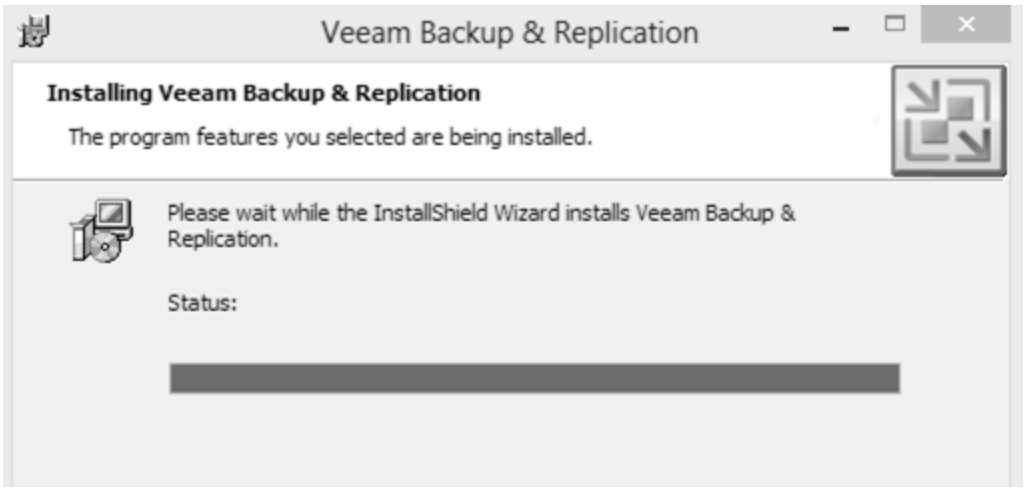


A następnie należy kliknąć Install.



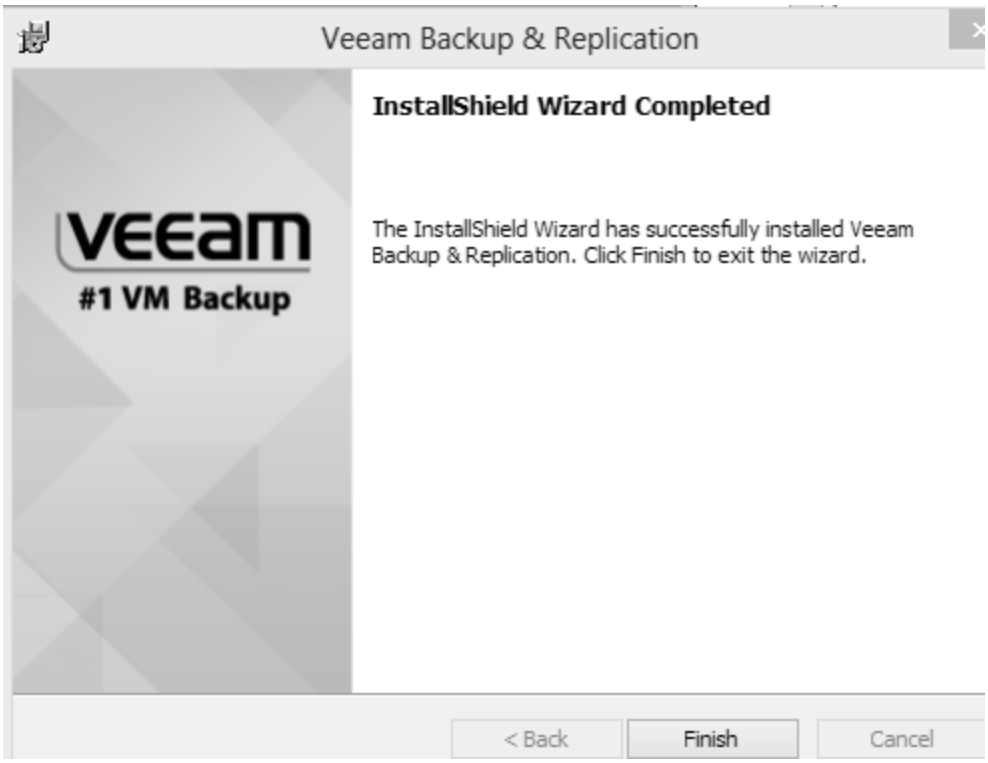
Teraz można obserwować postę instalacji.





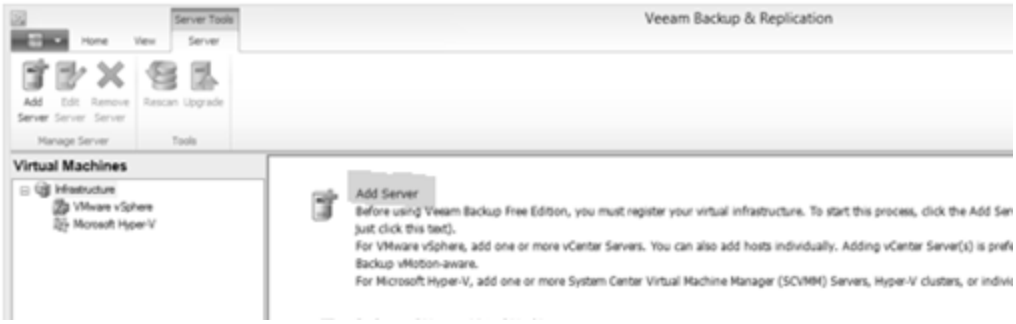
,

Gdy instalacja zostanie ukończona, należy kliknąć Finish.

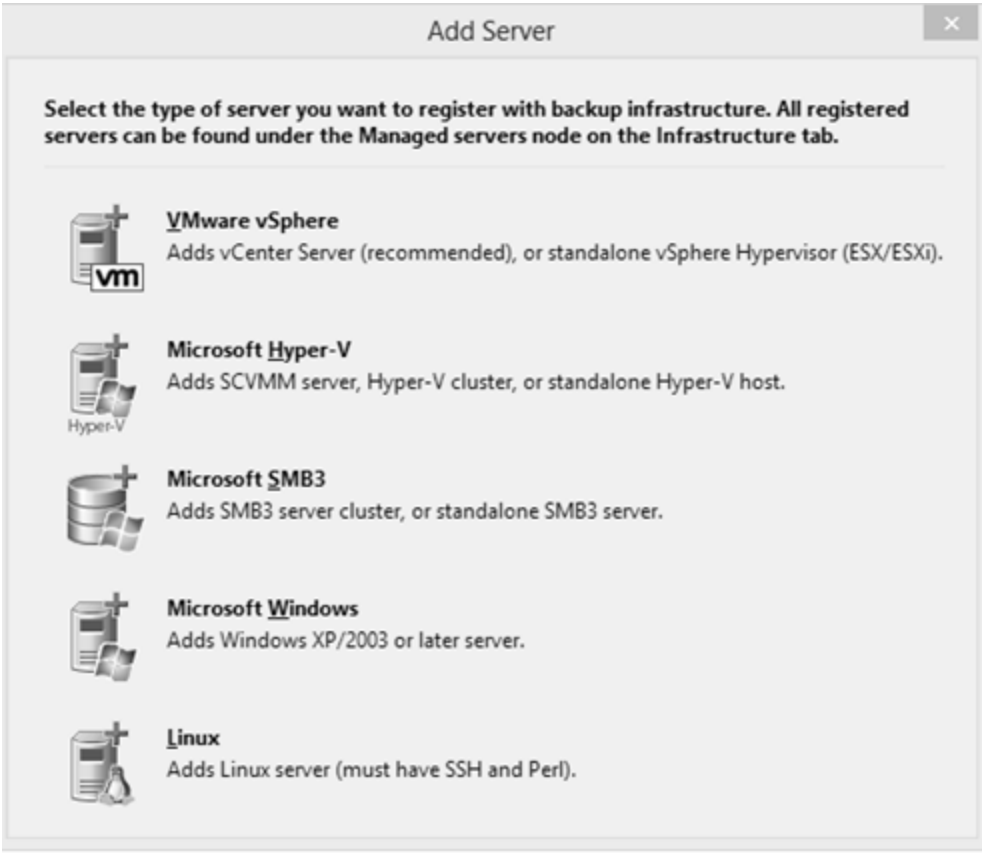


49.2. Dodawanie serwera do tworzenia kopii zapasowych

Należy rozpocząć od uruchomienia aplikacji Veeam Backup and Replication i kliknięcia Add server.

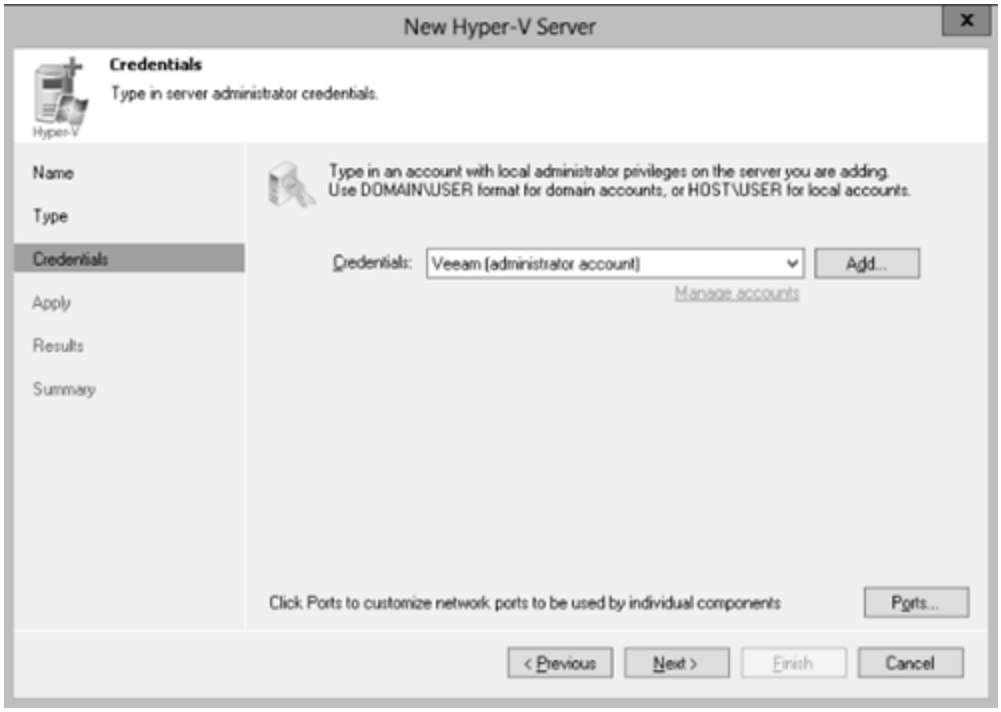


Teraz należy wybrać Hyper-V, VMWARE lub Windows Serwer, który chcemy skonfigurować do tworzenia kopii zapasowych. Wybieram serwer Hyper-V w celu demonstracji kopii zapasowych.

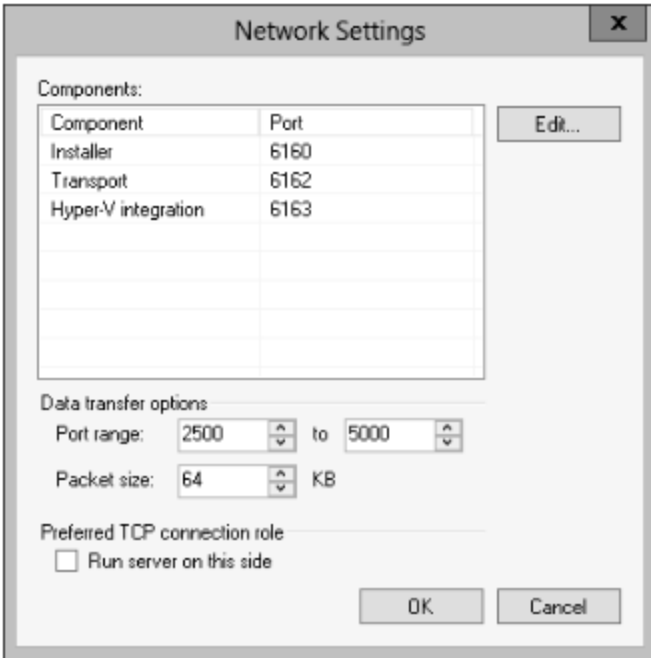


Należy wybrać, jeśli chcemy wykonać kopię zapasową SCVMM lub Hyper-V cluster lub Hyper-V standalone server i kliknąć Next.

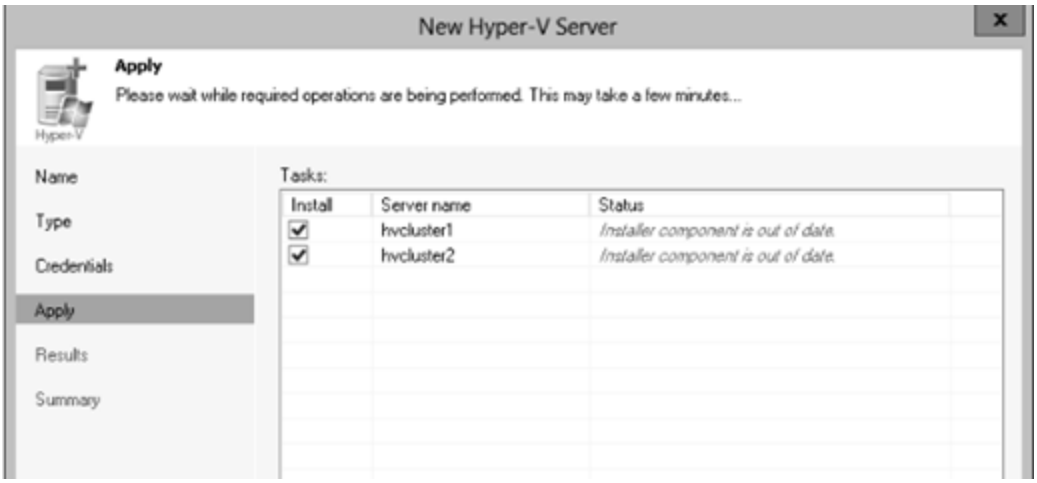
Następnie trzeba podać dane i kliknąć Ports, jeśli chcemy dostosować informacje o portach.



Dalej należy kliknąć OK i Next.

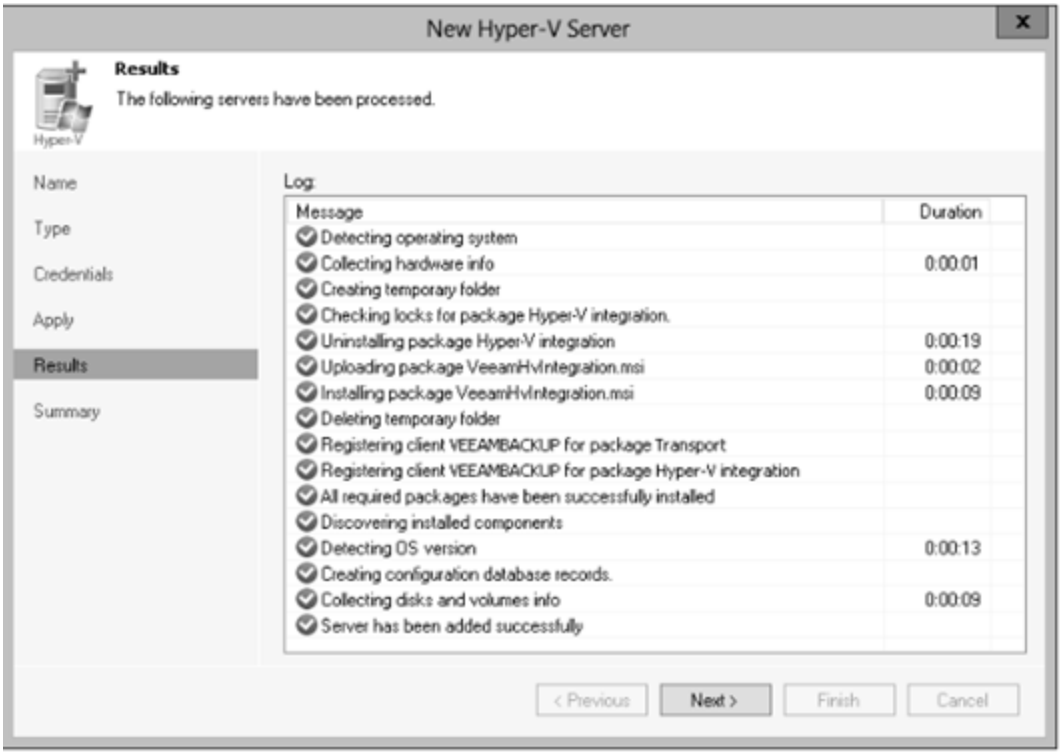


Następnie należy kliknąć Next na Confirming Backup Settings.

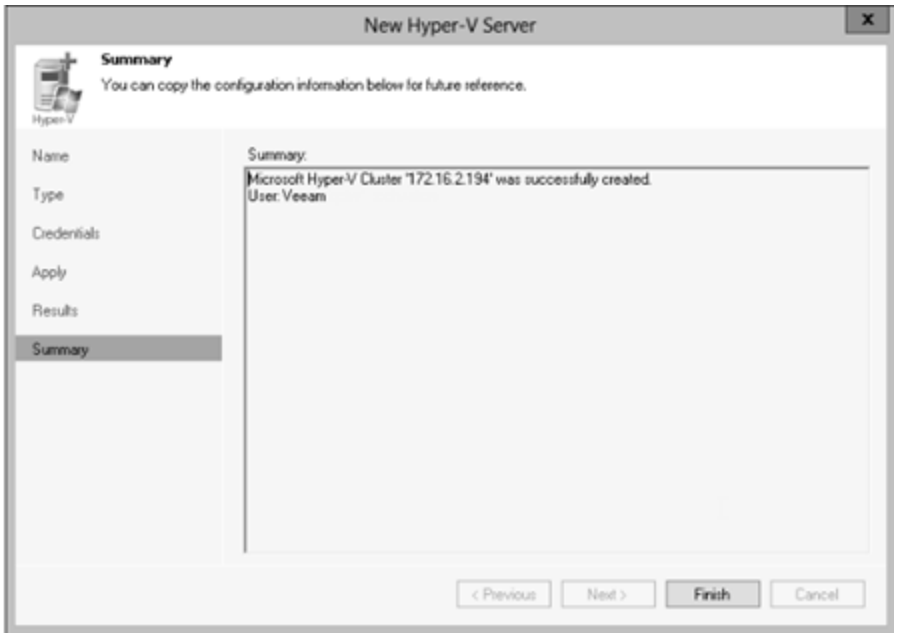


Jeśli dokonaliśmy wyboru standalone server, można skonfigurować maks. współbieżne zadania, które można uruchomić.

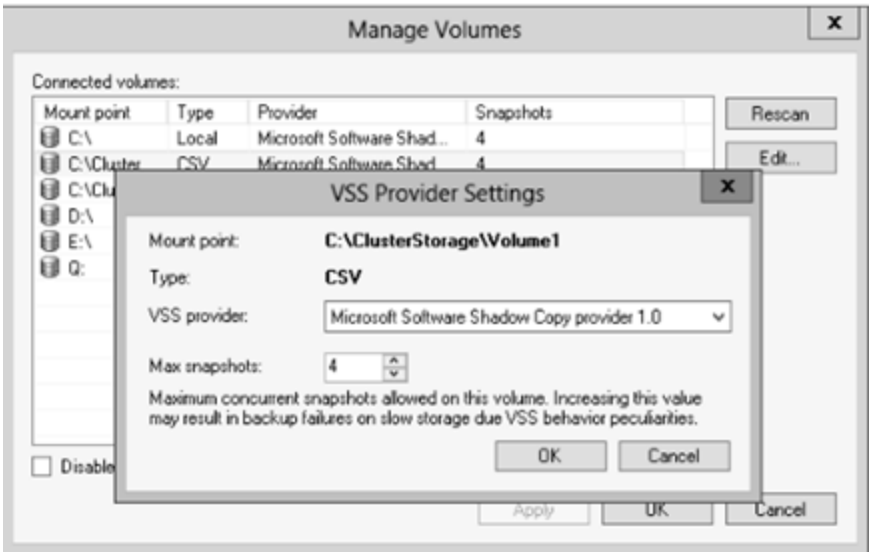
Kreator przeprowadzi weryfikację, po czym należy kliknąć Next.



Teraz należy kliknąć Finish.

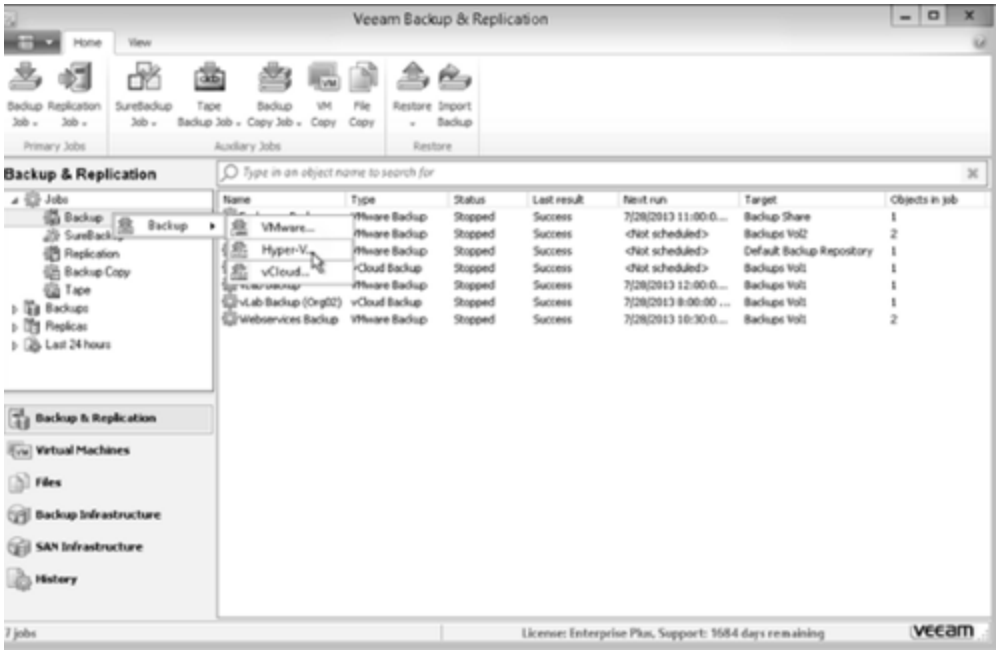


Po dodaniu serwera można skonfigurować ustawienia dla Volume backup z Manage Volumes.

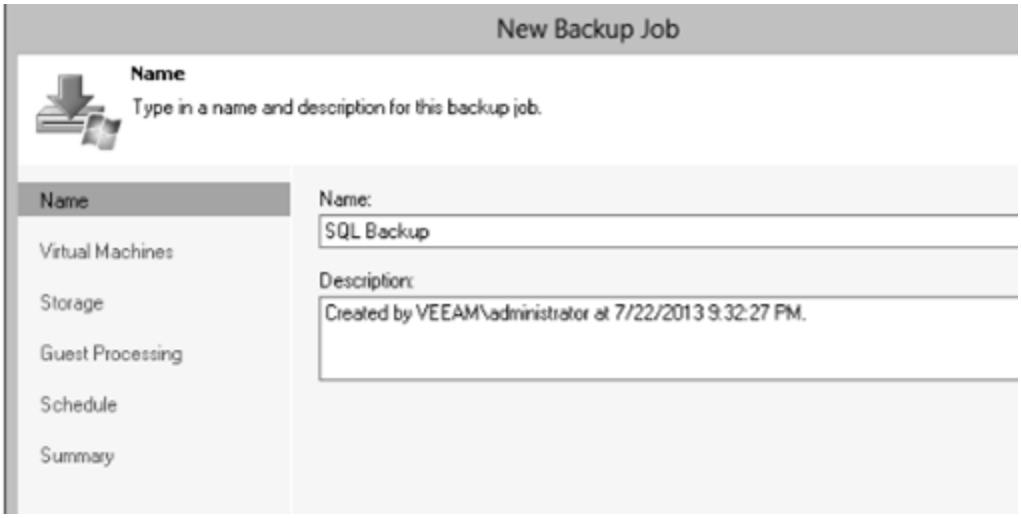


49.3. Tworzenie Backup Job

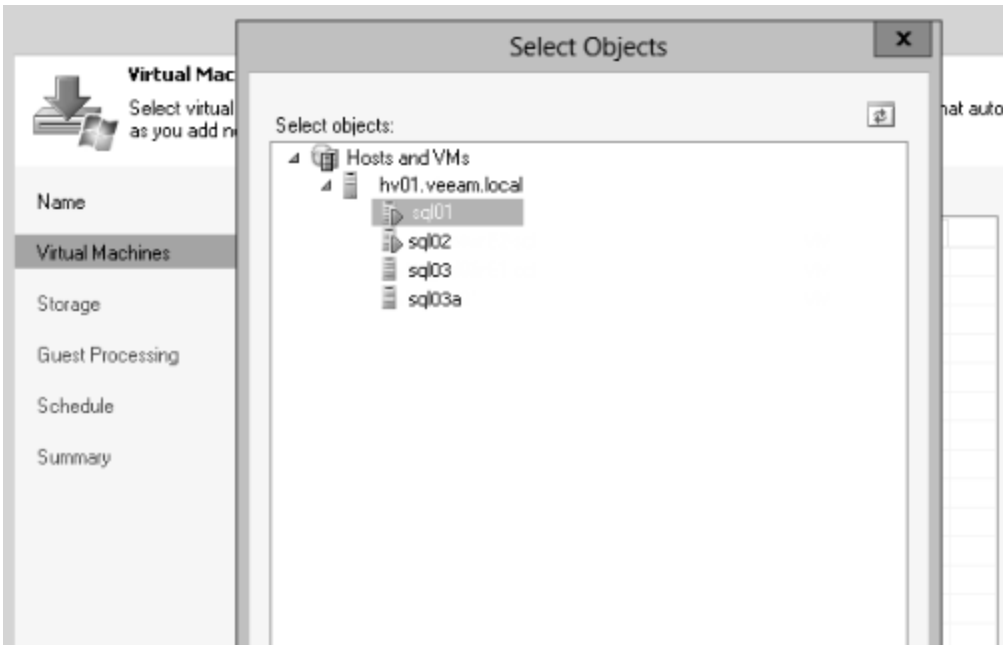
Na konsoli Veeam Backup and Replication należy kliknąć opcję backup and Hyper-V.



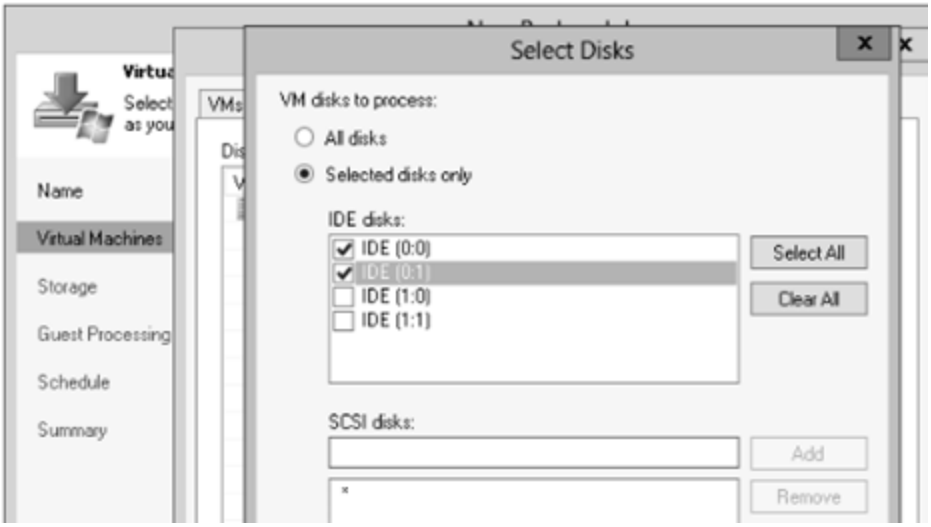
Teraz trzeba podać nazwę backup job i kliknąć Next.



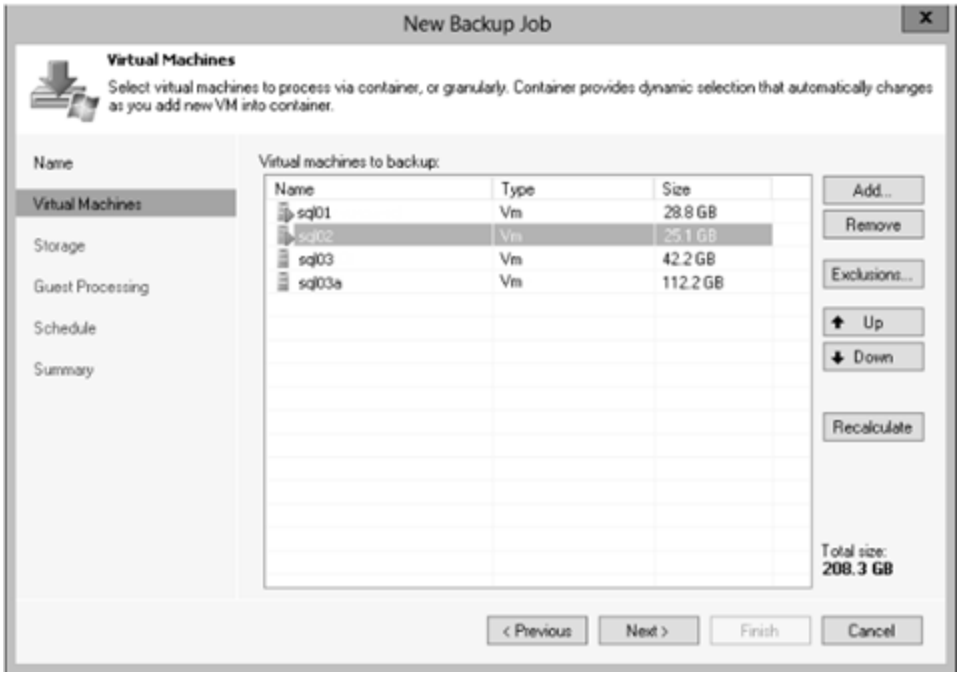
Następnie należy kliknąć Add -> Wybierz Maszyny wirtualne, dla których chcesz wykonać kopię zapasową i kliknąć OK.



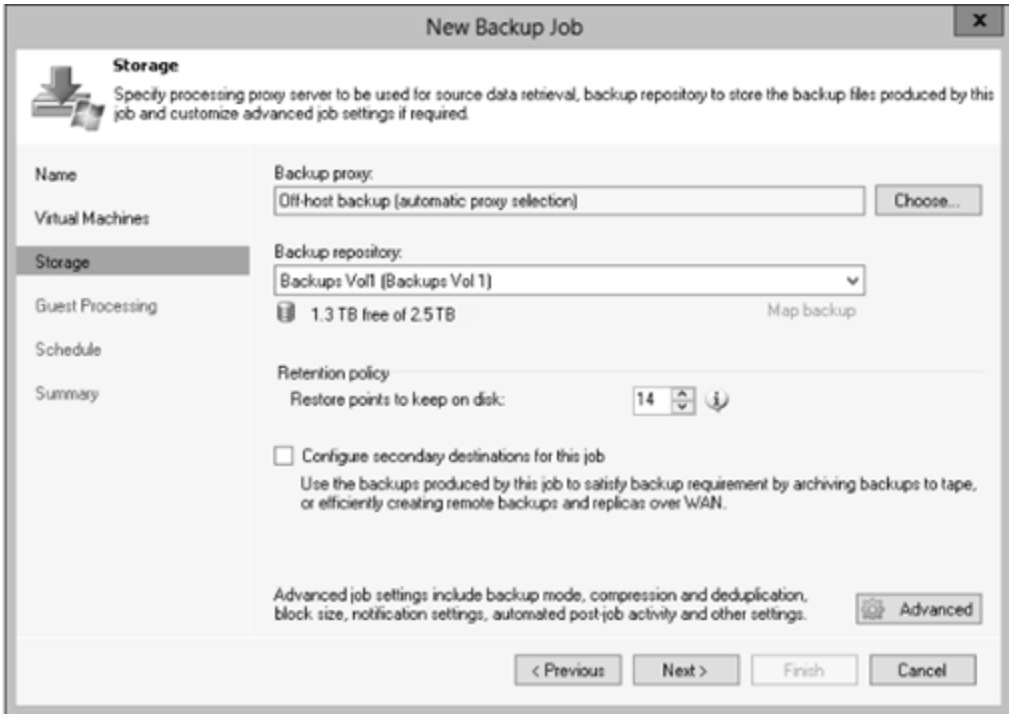
Dalej należy kliknąć Exclusions -> Exclude objects from backup job i kliknąć OK.



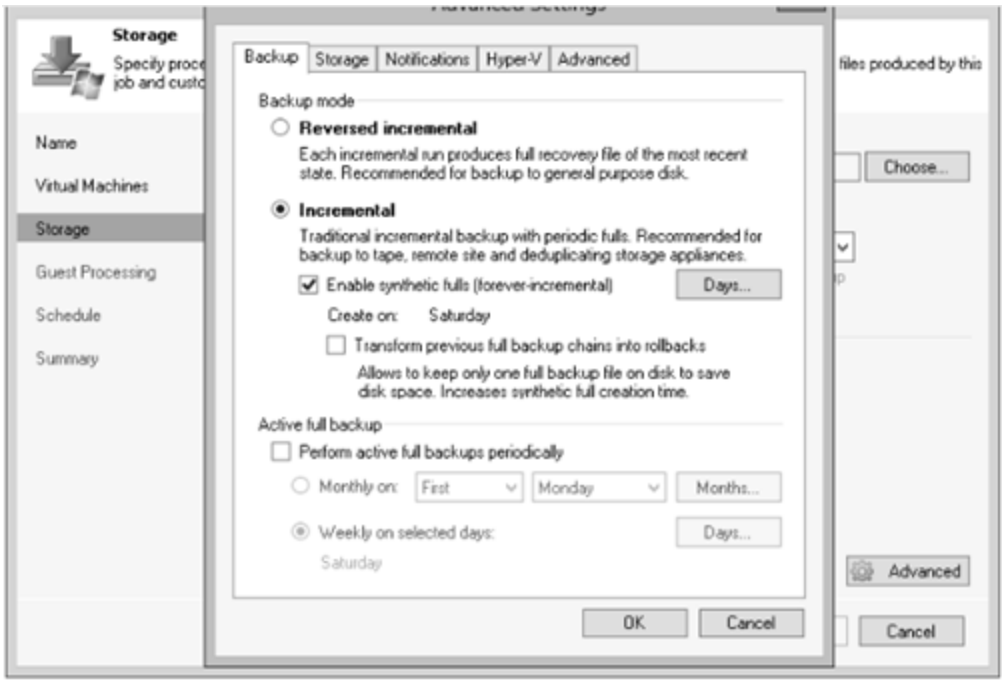
Należy zdefiniować kolejność kopii zapasowych i kliknąć Next.



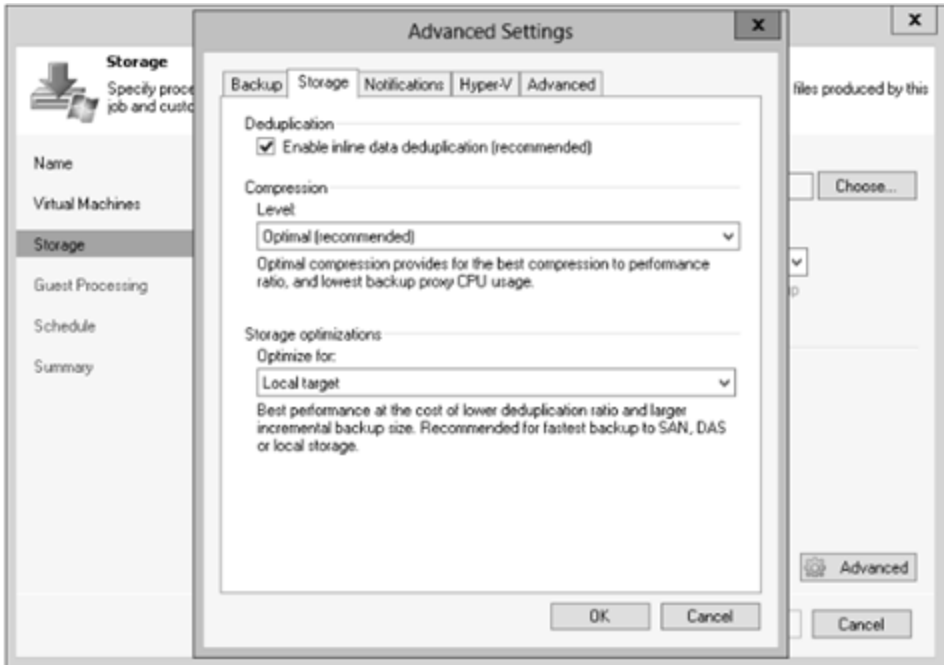
Teraz należy określić Backup storage i kliknąć Advanced.



Następnie należy określić ustawienia zaawansowane, czyli wybrać ustawienia, jakiego rodzaju kopii zapasowej potrzebujemy w zakładce Backup.

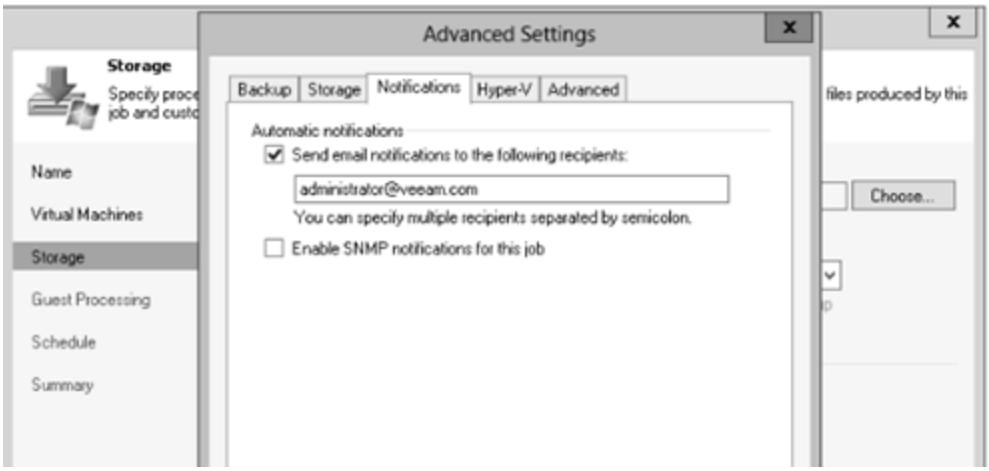


Na zakładce Storage należy określić opcje optymalizacji kompresji i pamięci.

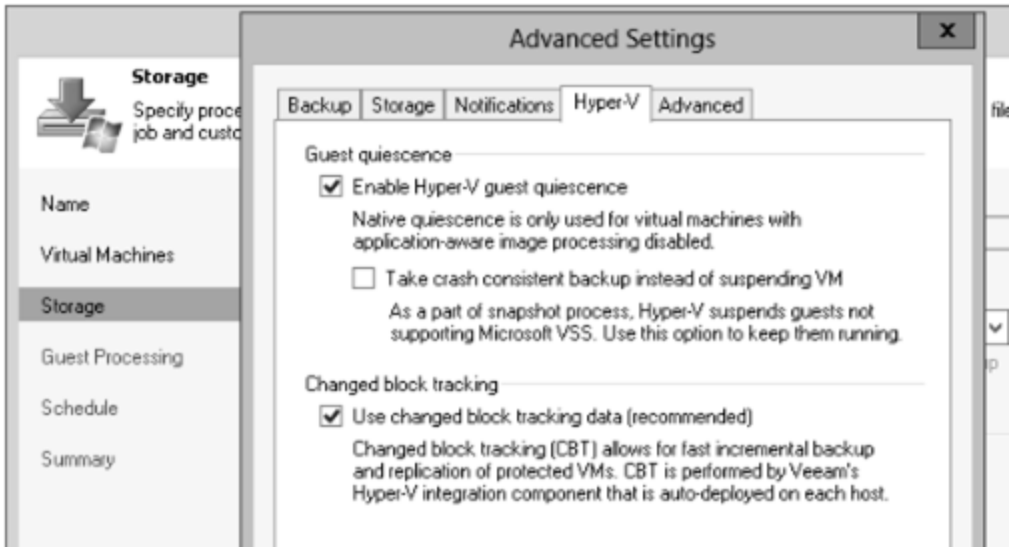


W zakładce Notification należy podać adres e-mail, do którego chcemy wysłać powiadomienie o stanie kopii

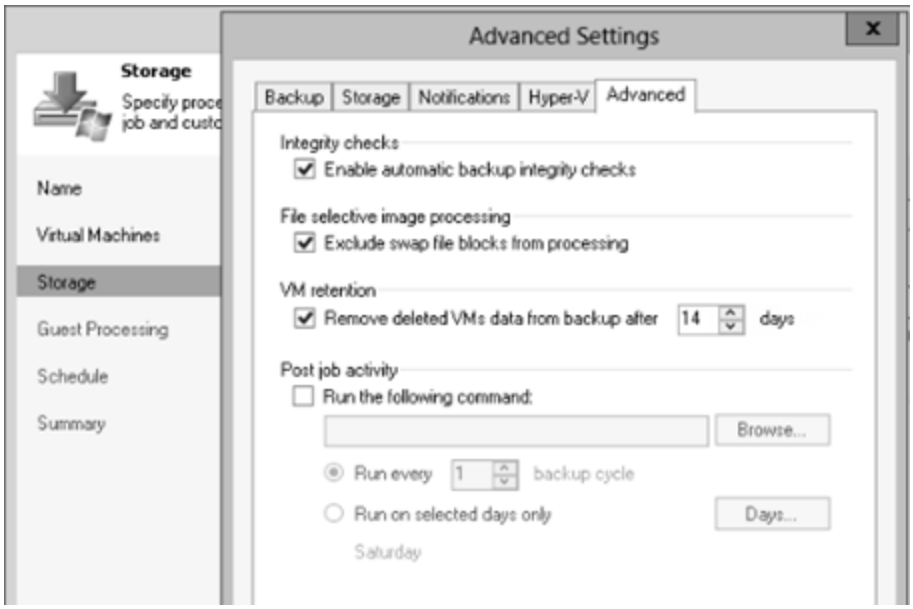
zapasowej.



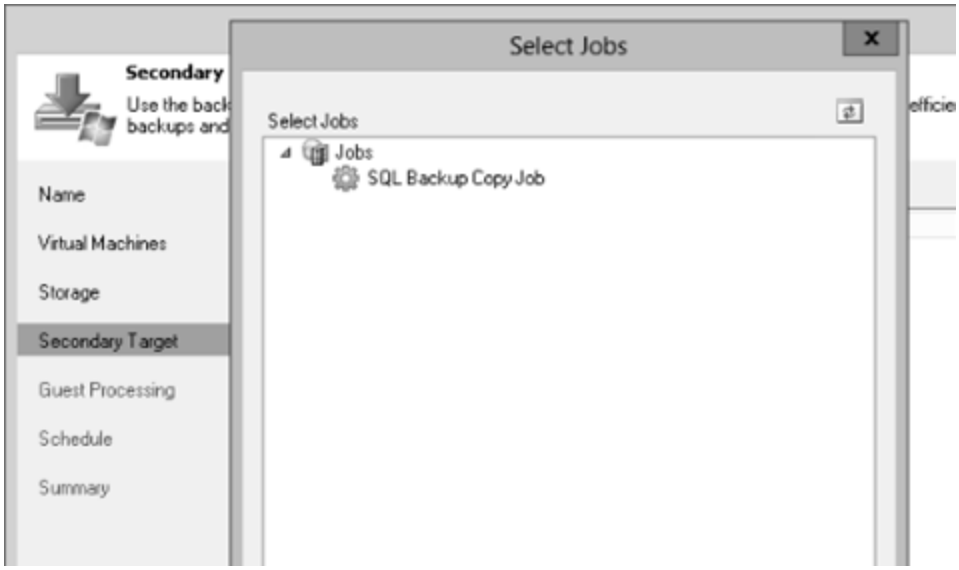
W zakładce Hyper-V należy zaznaczyć, jak na poniższym zrzucie z ekranu.



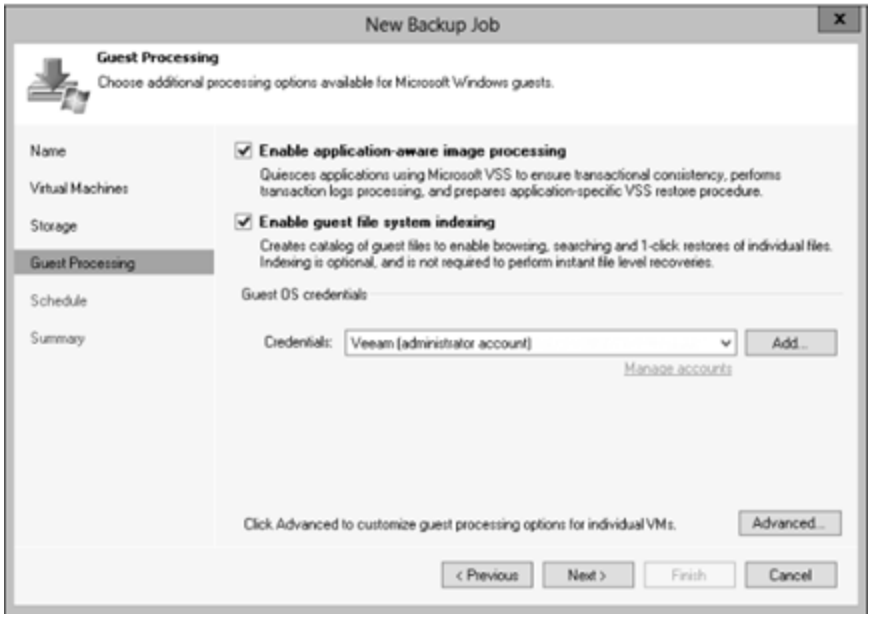
W zakładce Advanced trzeba określić kontrole integralności, przetwarzanie obrazu i opcje przechowywania VM.



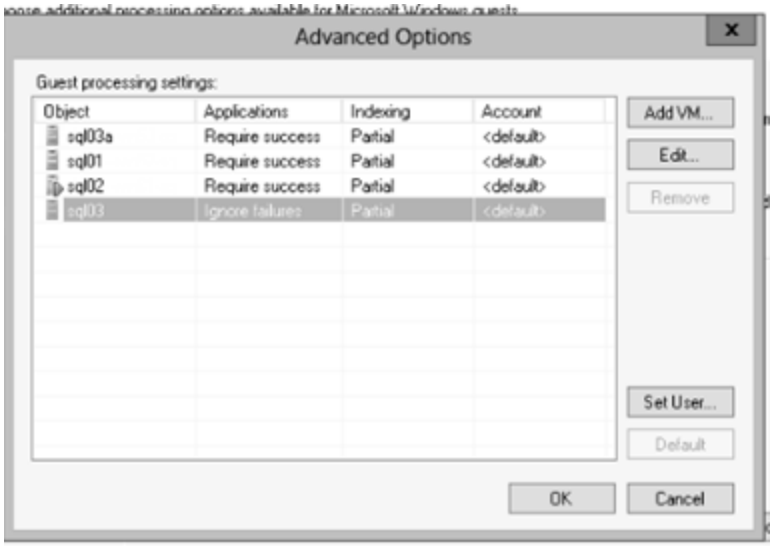
Jeśli chcemy określić jakiekolwiek post backup job, należy zaznaczyć pole Post Job activity i kliknąć Browse, a następnie zaznaczyć job i kliknąć OK.



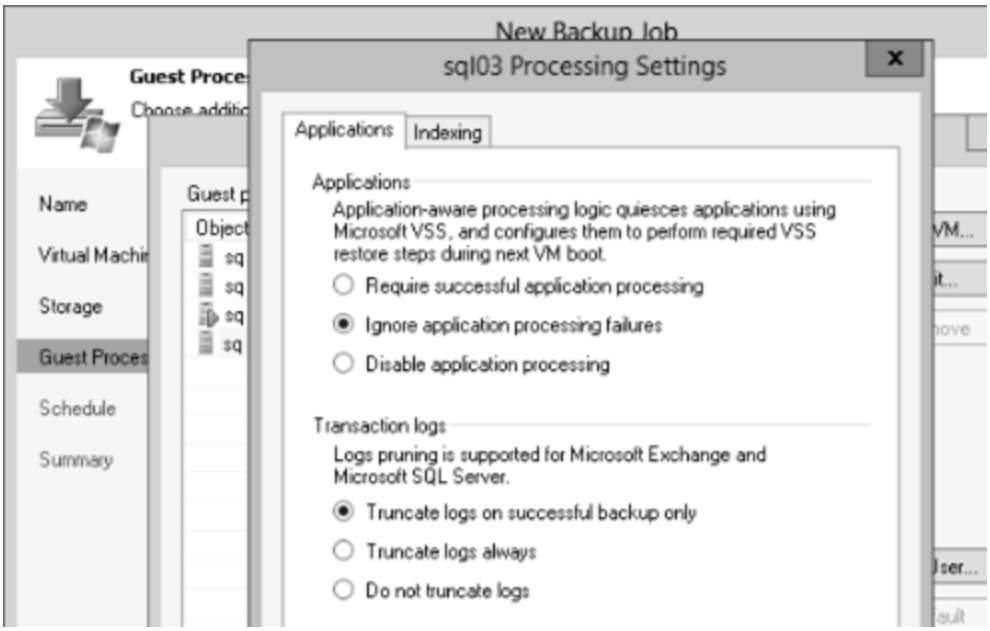
Teraz należy wybrać opcję Guest Processing i kliknąć Next.



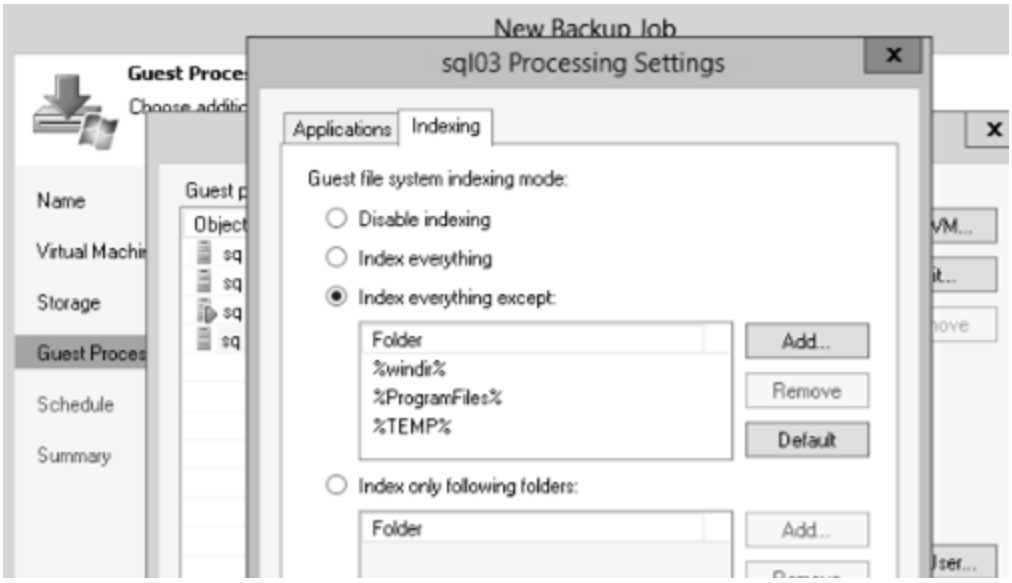
Następnie należy wybrać Advanced, aby edytować ustawienia guest processing, a później wybrać VM i kliknąć Edit.



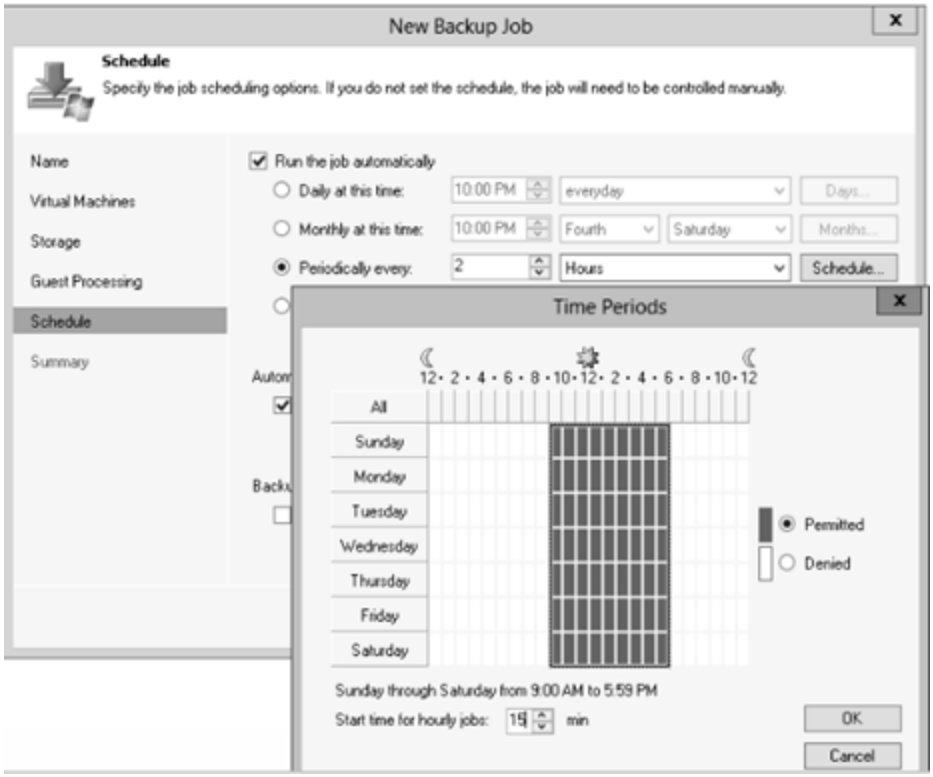
Dalej należy wybrać opcje na zakładce Application.



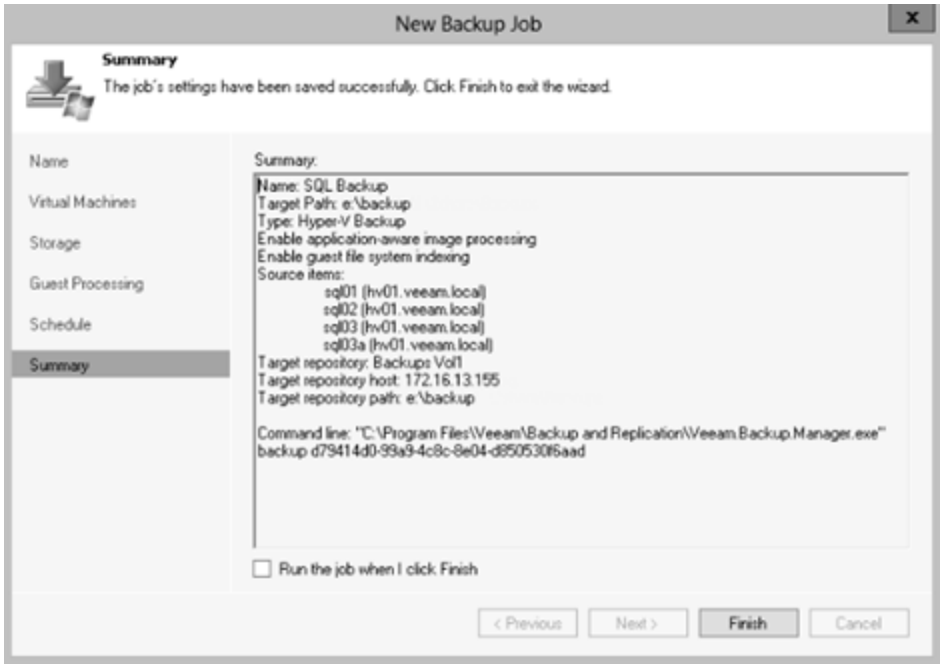
Następnie trzeba wybrać ustawienia w zakładce Indexing i kliknąć OK -> OK i Next.



Dalej należy wybrać harmonogram dla Backup Job i kliknąć Next.

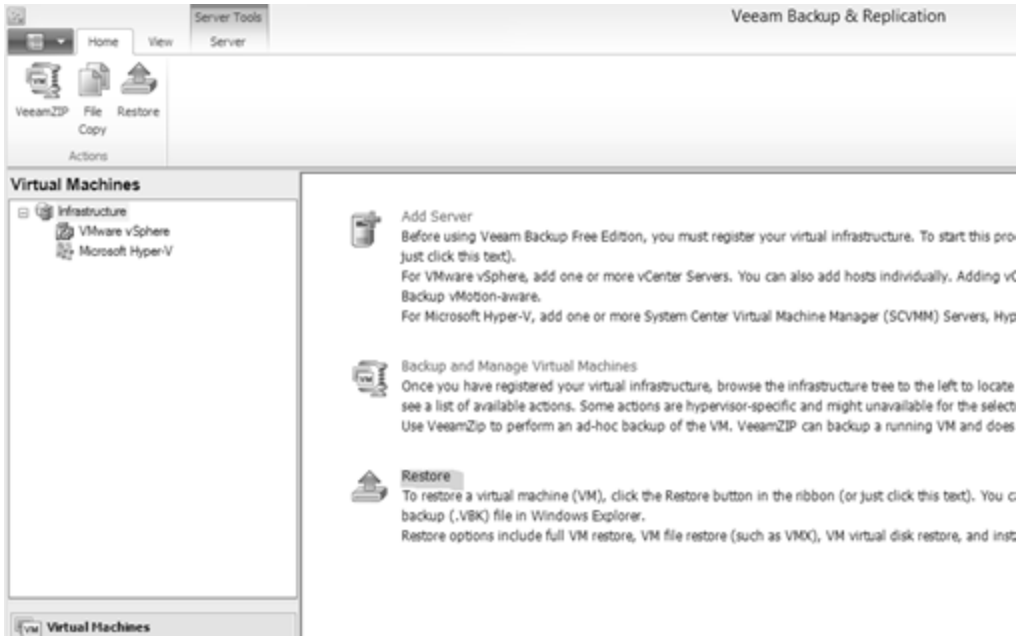


Teraz można już kliknąć Finish.

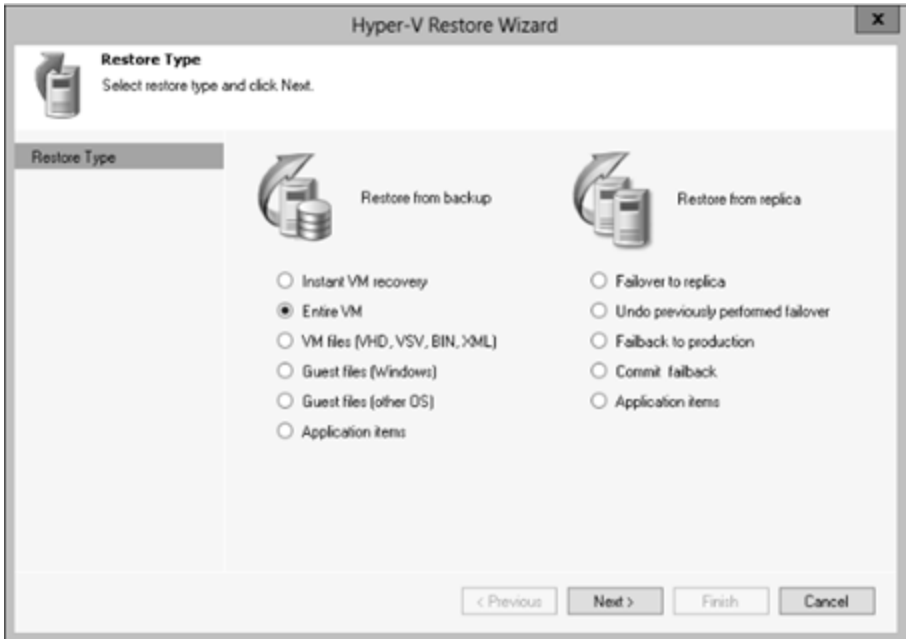


49.4. Wykonanie pełnego przywracania VM

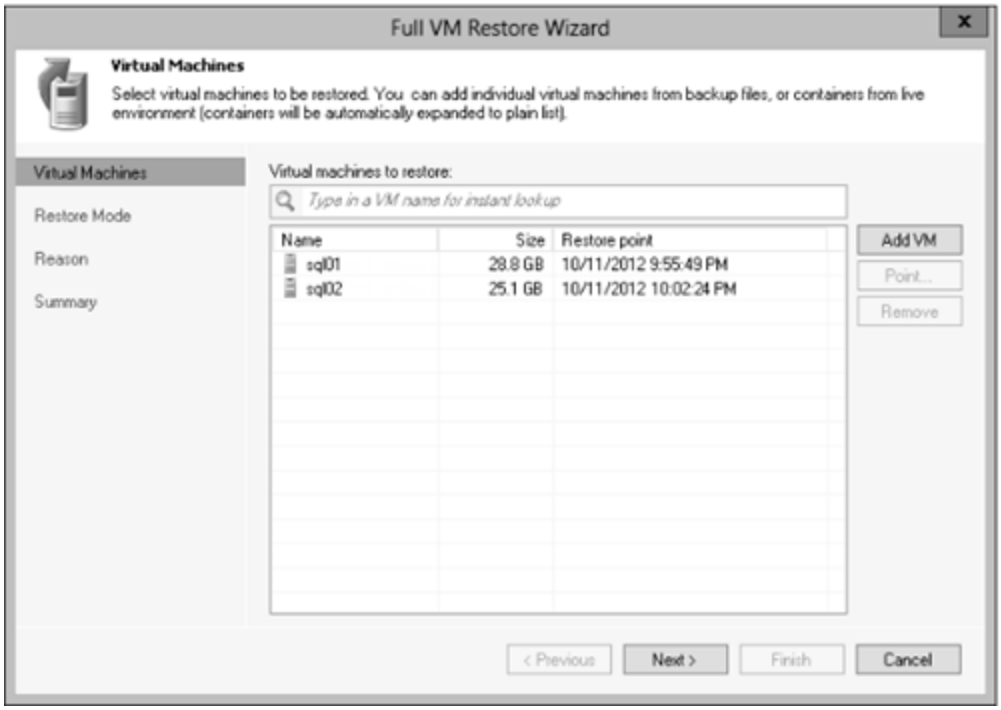
Z konsoli Veeam Backup and Replication należy wybrać opcję Restore.



Następnie należy wybrać typ przywracania i kliknąć Next.

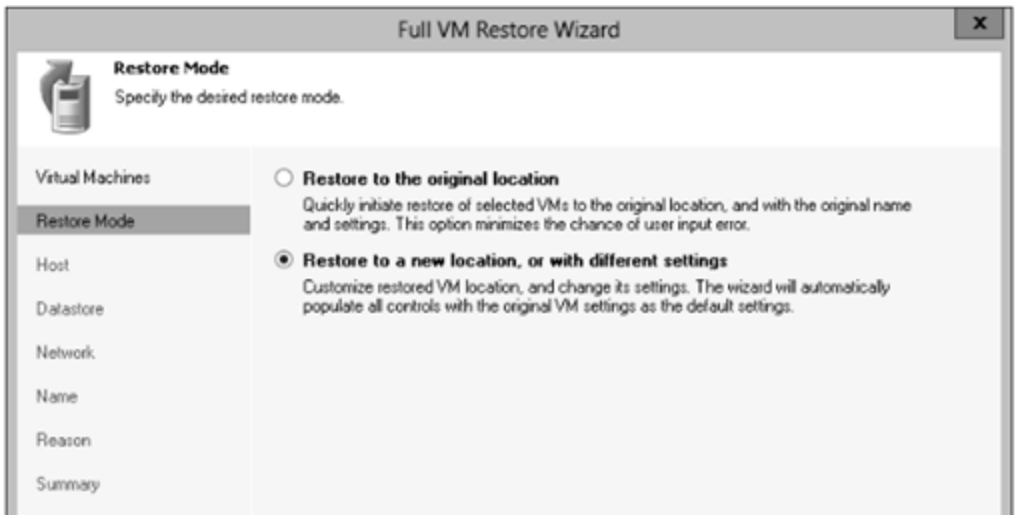


Dalej należy wybrać maszynę wirtualną, którą chcemy przywrócić.

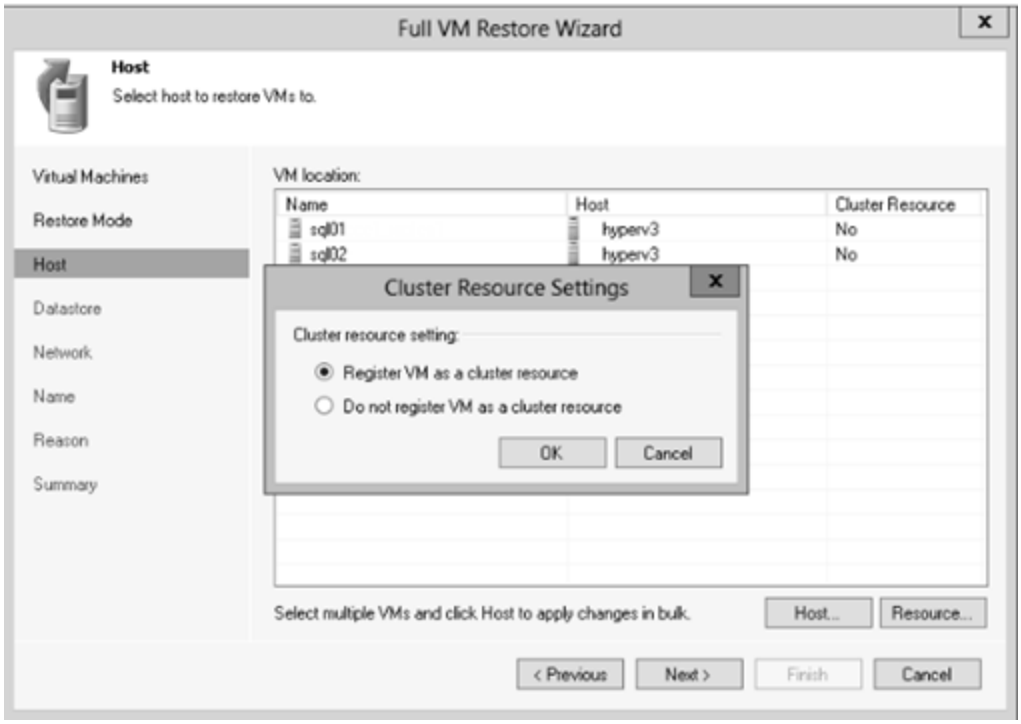


Teraz trzeba wybrać punkt przywracania do przywrócenia i kliknąć OK.

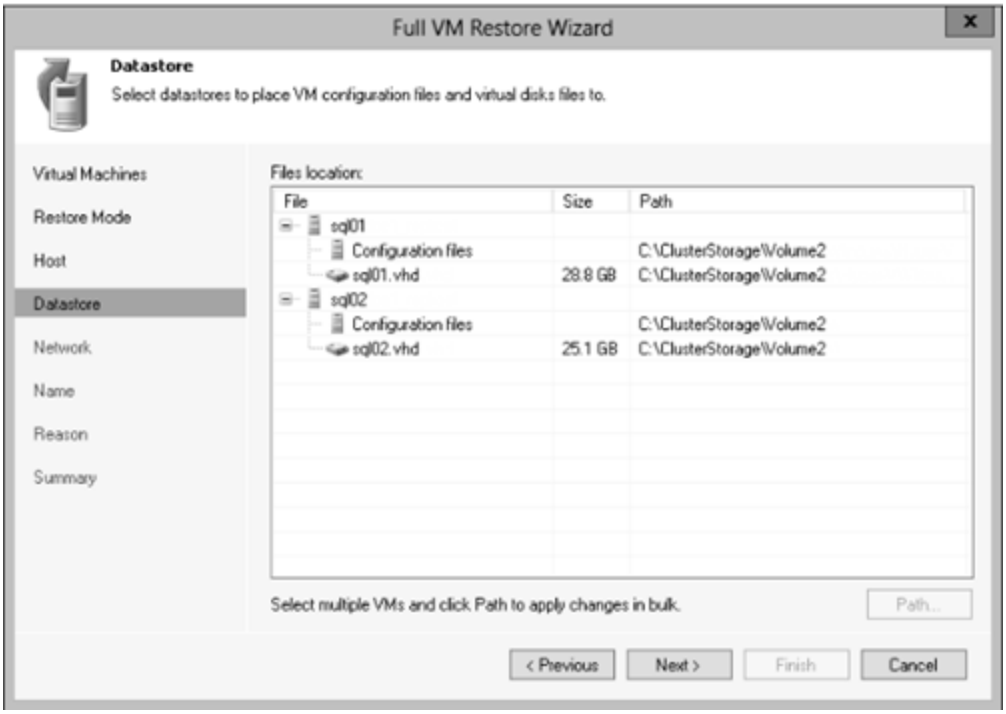
Następnie należy wybrać, czy chcemy przywrócić original location (oryginalna lokacja), czy new location (nowa lokacja).



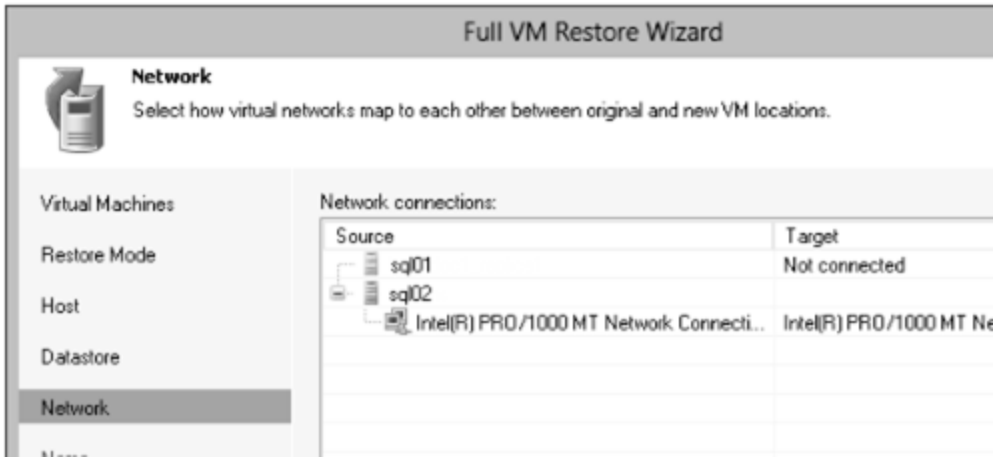
Dalej należy wybrać, czy przywrócona maszyna wirtualna będzie zasobem klastra, czy nie i kliknąć Next.



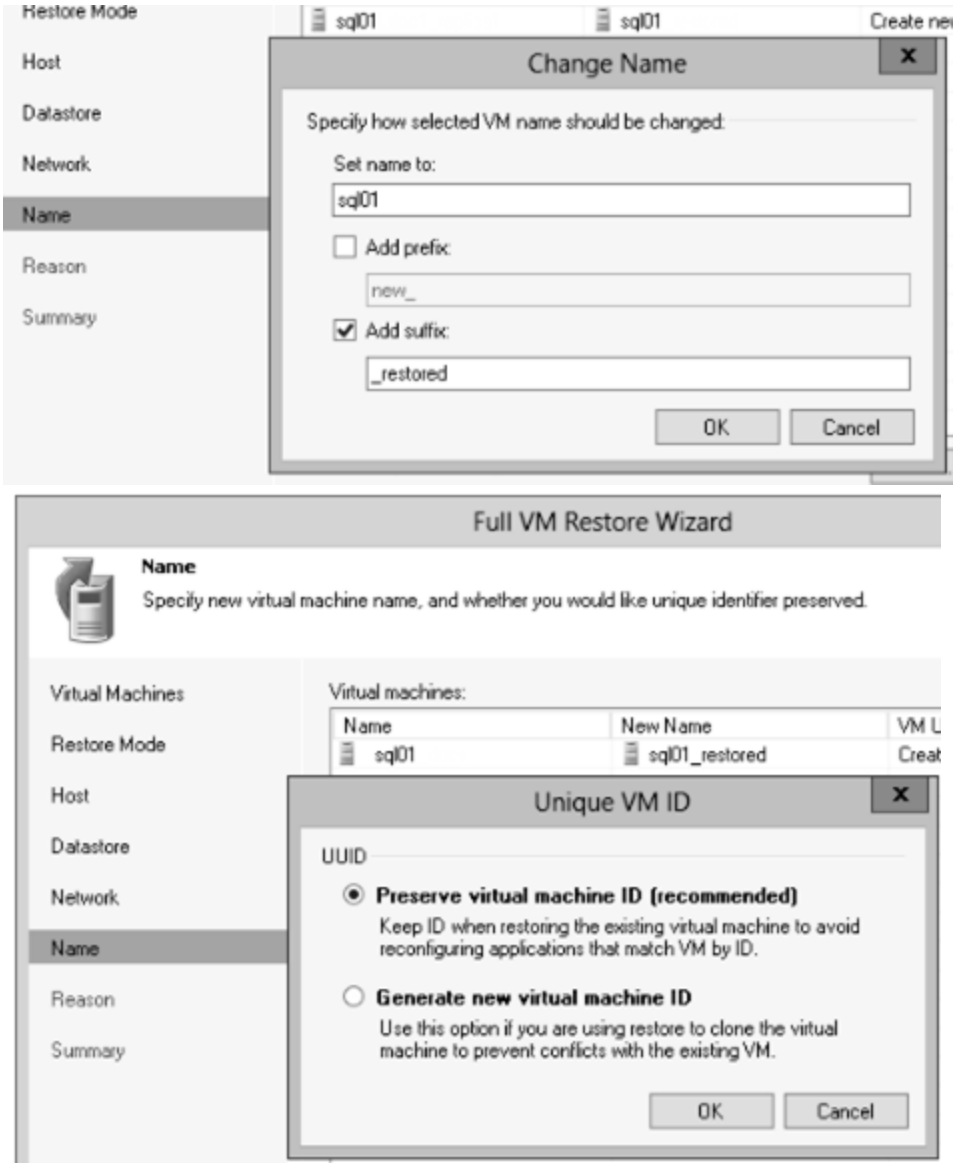
Można już wybrać magazyn danych, w którym chcemy przywrócić te pliki.



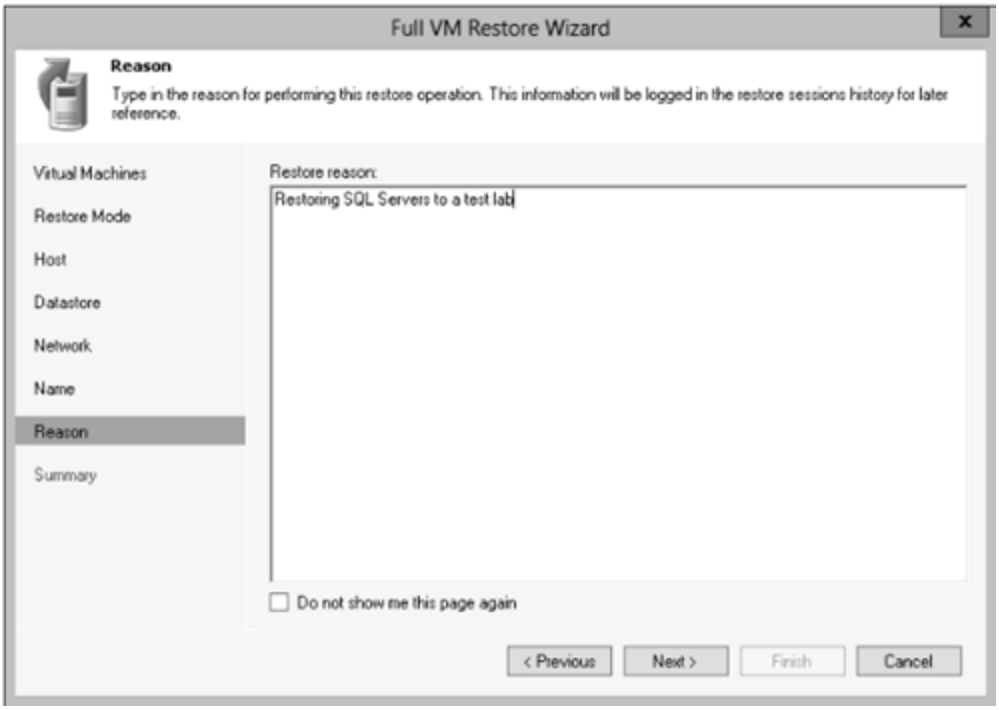
Następnie należy wybrać sposób odwzorowania środowiska wirtualnego między oryginalną i przywróconą maszyną wirtualną (na wypadek przywracania do innej lokalizacji).



Teraz należy określić nazwę maszyny wirtualnej i zadecydować, czy chcemy zachować identyfikatory.



Dalej należy wybrać przyczynę przywracania i kliknąć Next.



Można w końcu kliknąć Finish i rozpocznie się przywracanie.

50. Microsoft Azure

Windows Azure to kompleksowy zestaw usług, które umożliwiają szybkie tworzenie, wdrażanie i zarządzanie aplikacjami w globalnej sieci zarządzanych przez centra danych Microsoft

Windows Azure to podstawa do uruchamiania aplikacji i przechowywania danych w chmurze.

Windows Azure to otwarta i elastyczna platforma chmurowa, która umożliwia szybkie tworzenie, wdrażanie i zarządzanie aplikacjami w globalnej sieci zarządzanych

przez Microsoft centrów danych. Można budować aplikacje za pomocą dowolnego języka, narzędzia lub frameworka.

Windows Azure składa się z pięciu głównych części: Compute, Storage, the Fabric Controller, CDN, amd Connect.

Compute: uruchamia aplikacje w chmurze. Te aplikacje w dużej mierze widzą środowisko Windows Server, chociaż model programowania Windows Azure nie jest dokładnie taki sam, jak model on-line Windows Server.

Storage: przechowuje dane binarne i dane strukturalne w chmurze.

Fabric Controller: wdraża, zarządza i monitoruje aplikacje. Fabric controller obsługuje również aktualizacje oprogramowania systemowego na całej platformie.

Content Delivery Network (CDN): przyspiesza globalny dostęp do danych binarnych w magazynie Windows Azure, utrzymując buforowane kopie tych danych na całym świecie.

Connect: umożliwia tworzenie połączeń na poziomie IP między komputerami lokalnymi i aplikacjami Windows Azure.

Windows Azure zapewnia możliwości, takie jak Virtual Machine, Cloud Services, Web sites.

Dzięki wirtualnym sieciom prywatnym można wdrażać maszyny wirtualne w chmurze i grupować je razem, aby stanowiły część ich prywatnej sieci.

Można także połączyć się z siecią firmową (jeśli ją posiadamy) i ustanowić bezpieczny tunel VPN, aby łączyć maszyny działające we własnym środowisku korporacyjnym z wirtualnymi maszynami w chmurze – dzięki czemu będą wyglądać tak, jakby wszystkie były częścią jednej połączonej sieci.

Tak wiele elastyczności po stronie obliczeniowej, jak i po stronie sieci.

W Windows Azure Web Sites istnieje usługa zarządzana, której można używać do uruchamiania witryn internetowych i internetowych interfejsów API.

Umożliwia szybkie wstawianie aplikacji internetowych i stron internetowych w Internecie.

Usługi w chmurze to kolejny model, który wspieramy w budowaniu aplikacji.

Usługi w chmurze umożliwiają szerszy zestaw obciążeń niż witryny sieci Web w systemie Windows Azure, zapewniając jednocześnie bardziej zautomatyzowane zarządzanie niż maszyny wirtualne Windows Azure.

Umożliwia budowanie czegoś, co czasami nazywamy nieskończenie skalowalną aplikacją. Mogą obsługiwać od jednej do setek lub tysięcy oczywiście.

Obsługa nie tylko wdrożeń internetowych, ale także wielowarstwowych architektur, w których można mieć kombinację frontów, średnich poziomów, a także maszyn wirtualnych działających w ramach naszego rozwiązania.

Obsługuje zautomatyzowane zarządzanie aplikacjami, dzięki czemu jest naprawdę łatwe do wdrożenia, skalowania, izolowania i odzyskiwania po każdym typie awarii sprzętu. Oprócz obsługi automatycznych aktualizacji.

Każde środowisko, które odnosi się do stabilności działania, musi być zgodne z umowami o gwarantowanym poziomie usług. Platforma Windows Azure nie jest wyjątkiem. Podczas wdrażania dwóch lub większej liczby instancji ról w różnych domenach błędów i aktualizacji umowa SLA Microsoft Windows Azure zapewnia, że nasze role internetowe będą miały łączność zewnętrzną co najmniej 99,95% czasu. Kluczową kwestią do zrozumienia w czasie serwisowania jest wykorzystanie domen błędów i domen aktualizacji: co one reprezentują i jaki jest ich wpływ na ogólną platformę Windows Azure.

Fault Domains

Domeny uszkodzeń reprezentują fizyczną jednostkę awarii, bardzo ściśle związaną z fizyczną infrastrukturą zawartą w centrach danych, a podczas gdy fizyczne ostrze lub stojak można uznać za domenę błędu, nie ma

bezpośredniego odwzorowania jeden do jednego między tymi dwoma.

Po wdrożeniu aplikacji na platformie Windows Azure kontroler aplikacji Windows Azure jest odpowiedzialny za wdrożenie aplikacji w różnych domenach błędów, z gwarancją, że aplikacja będzie używać co najmniej dwóch domen błędów, a tym samym spełnia wymagania umowy SLA dla Windows Azure. Aby tak się stało, istnieje wymóg skonfigurowania wielu instancji usług ról aplikacji. Dystrybucja domen błędów to coś, nad czym nie mamy bezpośredniej kontroli, ale są sposoby, którymi można wpłynąć na ogólną dostępność naszej aplikacji.

Upgrade Domains

Domeny aktualizacji reprezentują jednostkę logiczną, która pomaga określić sposób aktualizacji roli w instancji. Kiedy nastąpi aktualizacja, Windows Azure przechodzi proces aktualizacji tych domen jeden po drugim. Domeny uaktualnień systemu Windows Azure chronią aplikację przed problemami prowadzącymi do potencjalnego przestoju.

Gdy ma miejsce żądanie aktualizacji, role otrzymują powiadomienie o zmianie. Wyobraź sobie, że masz 50 instancji roli, wszystkie otrzymały powiadomienie od razu, a wszystkie te instancje reagowały na powiadomienie o aktualizacji. Ten scenariusz prowadziłby do niedostępnych

ról i rywalizacji o zasoby, prowadząc do przestojów. Platforma Windows Azure będzie chronić przed wezwaniami do zalewania, aby uaktualnić daną usługę do nowej wersji do wdrożenia.

51. Kontenery Docker w Windows Server

Gdy zacznie się pracować z kontenerami, można zauważyć wiele podobieństw między kontenerem a maszyną wirtualną; ale w rzeczywistości są to dwie zupełnie różne koncepcje. Kontenery zmienią sposób, w jaki będziemy pracować nad systemem Windows. Nicolas Prigent wyjaśnia, jak korzystać z funkcji Windows Containers.

Kontenery systemu Windows zrewolucjonizują wirtualizację i proces DevOps.

W systemie Windows Server 2016 firma Microsoft wprowadza nową funkcję o nazwie Kontenery Windows. Organizacje, które aktualizują swoje serwery do tego nowego systemu operacyjnego, będą mogły korzystać z kontenerów od etapu projektowania do środowiska produkcyjnego.

Robert Sheldon napisał świetny artykuł o kontenerach Windows na Simple Talk: https://www.simple-talk.com/cloud/platform-as-a-service/windows-containers-and-docker/. Nie będziemy jeszcze raz zagłębiać się w koncepcję kontenerów, ale w tym dziale wyjaśnię, jak

tworzyć, uruchamiać, konwertować i zarządzać kontenerami Windows.

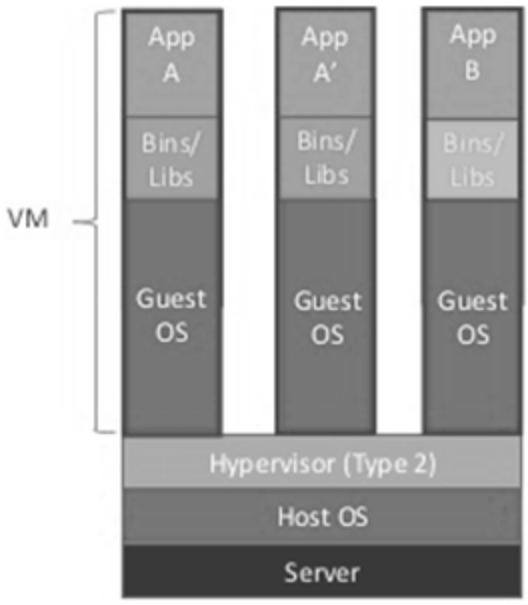
51.1. Podstawy kontenerów systemu Windows

Zanim zacznę od praktycznej strony Windows Containers, powinienem szybko omówić podstawy dotyczące tej nowej funkcji.

Kontenery owijają oprogramowanie w kompletny system plików, który zawiera wszystko, czego potrzebuje do działania: kod, środowisko wykonawcze, narzędzia systemowe i biblioteki systemowe. Gwarantuje to, że zawsze będzie działać tak samo, niezależnie od środowiska, w którym działa. Aby osiągnąć ten cel, system Windows wykorzystuje izolację przestrzeni nazw, kontrolę zasobów i technologie izolacji procesów, aby ograniczyć pliki, porty sieciowe i uruchomione procesy, do których każdy kontener może uzyskać dostęp, aby aplikacje działające w kontenerach nie mogły wchodzić w interakcje ani wyświetlać innych działających aplikacji w systemie hosta lub w innych kontenerach.

Wirtualne Maszyny vs Kontenery

Maszyna wirtualna jest samodzielna i ma własny system operacyjny, własne aplikacje i własne zasoby (pamięć, procesor itd.). Poniższy schemat pokazuje trzy maszyny wirtualne hostowane na tym samym hoście fizycznym. Każda maszyna wirtualna korzysta z własnego systemu operacyjnego, bibliotek itp. W konsekwencji zajmują one znaczną część pamięci.



Architektura Wirtualnych Maszyn

Dość często programiści muszą bardzo szybko testować aplikacje o różnych wersjach. Następnie muszą poprosić zespół IT Ops o wdrożenie jednej lub wielu maszyn (Virtual lub Physical). Jest to czasochłonny proces. Maszyny

wirtualne zużywają również znaczne zasoby, takie jak pamięć i przestrzeń dyskowa. Z tego powodu kontenery są niesamowicie przydatne w procesie DevOps.

Architektura Kontenerów

Kontenery nie zawierają żadnego systemu operacyjnego, więc pobierają mniej zasobów niż maszyny wirtualne na hoście fizycznym. Kontenery po prostu współdzielą system operacyjny hosta, w tym jądro i biblioteki, dzięki czemu nie muszą uruchamiać pełnego systemu operacyjnego.

Podsumowując, zalety kontenerów systemu Windows są następujące:

- Podczas wdrażania kontenera w środowisku produkcyjnym proces wycofywania jest bardzo prosty. Wystarczy zmodyfikować skrypt wdrażania i ponownie wdrożyć obraz kontenera. Po prostu można sobie wyobrazić proces wycofywania z maszyn wirtualnych. Cóż, należy przebudować całą maszynę (lub przywrócić poprzednią migawkę / kopię zapasową).

- Czas uruchomienia kontenera Windows jest szybszy niż maszyna wirtualna.
- Scenariusz oparty na chmurze ma niewielkie rozmiary.

Na zakończenie, filozofia pojemnika to „jedna usługa na pojemnik”.

Kontenery Windows Server vs Kontenery Hyper-V

Microsoft zawiera dwa różne typy kontenerów. Pierwszy typ oparty jest na obrazie Windows Server Core i nosi nazwę Windows Server Container. Drugi nazywa się Hyper-V Container i opiera się na obrazie Windows Nano Server. Kontenery Hyper-V rozszerzają izolację zapewnianą przez kontenery systemu Windows Server, uruchamiając każdy kontener na wysoce zoptymalizowanej maszynie wirtualnej, dzięki czemu zapewniają pełną izolację. Jądro hosta kontenera nie jest współdzielone z innymi kontenerami Hyper-V. Jeśli cały kod działający na hoście jest zaufany, izolacja zapewniona przez Windows Containers prawdopodobnie będzie odpowiednia. Ale jeśli nie ufamy kodowi, to Hyper-V Containers zapewniają taki sam poziom izolacji, jak maszyny wirtualne, ale z wieloma zaletami standardowych kontenerów.

Należy pamiętać, że kontenery Hyper-V są zarządzane tylko przez Docker, natomiast maszyny wirtualne Hyper-V są zarządzane przez tradycyjne narzędzia, takie jak Hyper-V Manager. W praktyce uruchamianie kontenerów Hyper-V trwa dłużej niż Windows Server Containers, ale oba są znacznie szybsze niż maszyny wirtualne z pełnym systemem operacyjnym (nawet na serwerze Nano).

Docker

W październiku 2014 roku Microsoft Corp i Docker ogłosiły partnerstwo strategiczne, aby zapewnić elastyczność, przenośność i bezpieczeństwo platformy Docker dla systemu Windows Server.

Windows Server 2016 Containers, obsługiwany przez silnik Docker

Konieczne jest zrozumienie, że Windows Server 2016 nie może uruchamiać kontenerów Linux w formacie Docker, a jedynie kontenery Windows. Dlaczego? Ponieważ kontenery linuksowe wymagają interfejsów API systemu Linux z jądra hosta, a kontenery systemu Windows Server

wymagają interfejsów API systemu Windows z jądrem systemu Windows.

Jednak proces zarządzania kontenerami Linux i Windows jest ściśle identyczny. Poniższy schemat opisuje platformę Docker:

Platforma Docker

Oto podsumowanie żargonu Windows Containers z ich znaczeniem:

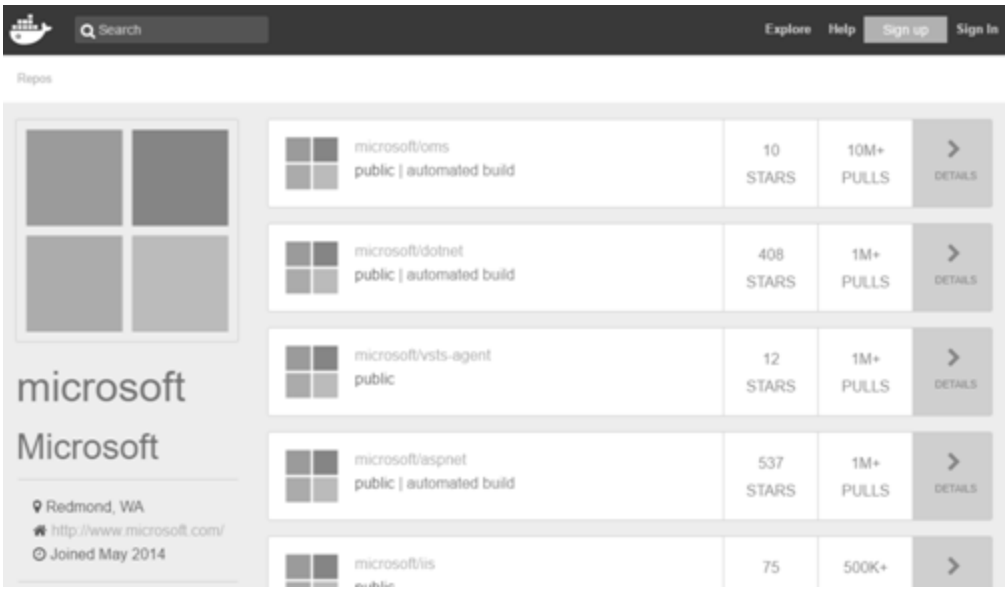
- Host kontenera: fizyczny lub wirtualny system komputerowy skonfigurowany z funkcją Windows Container.

- Obraz kontenera: obraz kontenera zawiera podstawowy system operacyjny, aplikację i wszystkie zależności aplikacji, które są potrzebne do szybkiego wdrożenia kontenera.
- Obraz OS kontenera: obraz systemu kontenera to środowisko systemu operacyjnego.
- Rejestr kontenerów: obrazy kontenerów są przechowywane w rejestrze kontenerów i można je pobrać na żądanie. Jest to miejsce, w którym publikowane są obrazy kontenerów. Rejestr może być zdalny lub lokalny.
- Silnik Docker: jest podstawą platformy Docker. Jest to lekkie środowisko wykonawcze kontenerów, które buduje i uruchamia kontener.
- Plik Docker: pliki Docker są używane przez programistów do budowania i automatyzowania tworzenia obrazów kontenerów. W przypadku pliku Docker demon Docker może automatycznie utworzyć obraz kontenera.

Docker zapewnia centralne repozytorium o nazwie Docker Hub (https://hub.docker.com/), publiczny rejestr konteneryzowanych aplikacji, który utrzymuje Docker. Obrazy kontenerów mogą być publikowane bezpośrednio w tym repozytorium, aby można je było udostępniać społeczności Docker. W Docker Hub jest już wiele obrazów, np:

- SQL,
- WordPress,
- IIS.

Można uruchomić prywatne repozytorium na miejscu. Firma Microsoft ma własne publiczne i oficjalne repozytorium dostępne za pośrednictwem tego adresu URL: https://hub.docker.com/u/microsoft/.



Kontenery Windows w praktyce

Przed wdrożeniem Windows Containers należy przygotować środowisko z pewnymi wymaganiami wstępnymi. Aby to zrobić, można użyć maszyny fizycznej lub wirtualnej, to zależy od nas. W moim przypadku używam maszyny wirtualnej o następujących cechach:

- System z systemem Windows Server 2016 (lub Windows 10). Jest to najważniejszy warunek wstępny. Radzę pracować z wersją Datacenter z powodu licencji (więcej informacji na końcu artykułu). Można wybrać

system Windows Server Core dla hosta kontenera, w przeciwieństwie do wersji systemu Windows, która zawiera pełny interfejs użytkownika.

- Uprawnienia administratora na hoście kontenera.
- Minimalna wolna przestrzeń dyskowa do przechowywania obrazów i skryptów wdrażania.
- Nasz serwer musi być aktualny.

OK, można zacząć od zainstalowania funkcji Windows Containers na hoście kontenera. Aby wykonać to zadanie, należy uruchomić następujące polecenie PowerShell:

```
PS C:\Users\Administrator> Install-WindowsFeature Containers

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    Yes            SuccessRest... {Containers}

WARNING: You must restart this server to finish the installation process.
```

Należy ponownie uruchomić, aby zastosować zmiany za pomocą polecenia Restart-Computer:

```
PS C:\Users\Administrator> Restart-Computer
```

Następnie sprawdź trzeba sprawdzić, czy nowa funkcja jest włączona:

PS C:\Users\Administrator> Get-WindowsFeature containers

Display Name Name Install State

----------- ---- ------------

[X] Containers Containers Installed

Kontenery systemu Windows są ściśle powiązane z Dockerem; należy zainstalować silnik Docker na hoście kontenera. Aby osiągnąć ten cel, mamy dwie możliwości:

Pierwszą z nich jest wdrożenie Docker z repozytorium.

PS C:\Users\Administrator> Install-Module -Name DockerMsftProvider -Repository PSGallery -Force

NuGet provider is required to continue

PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet

provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or

'C:\Users\Administrator\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by

running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install

and import the NuGet provider now?

[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"):

Jeśli potrzeba więcej informacji na temat zarządzania pakietami za pomocą PowerShell, polecam ten artykuł:

https://www.simple-talk.com/sysadmin/powershell/managing-packages-using-windows-powershell/

PS C:\Users\Administrator> Install-Package -Name docker -ProviderName DockerMsftProvider

The package(s) come(s) from a package source that is not marked as trusted.

Are you sure you want to install software from 'DockerDefault'?

[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y

Install-Package : KB3176936 or later is required for docker to work

At line:1 char:1

+ Install-Package -Name docker -ProviderName DockerMsftProvider

+ ~~~~~~

+ CategoryInfo : InvalidOperation: (Microsoft.Power....InstallPackage:InstallPackage) [Install-Package],

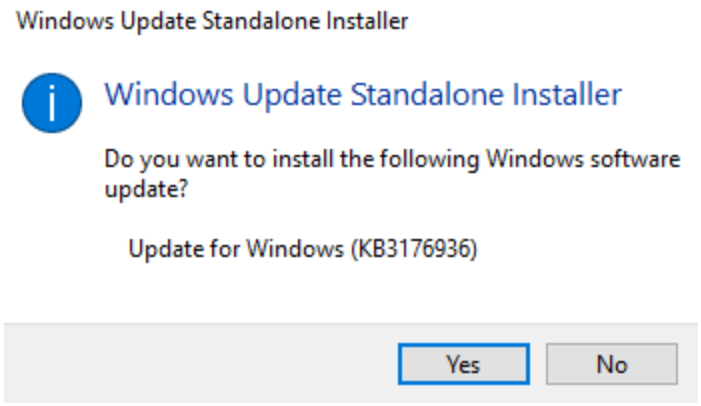
Exception

+ FullyQualifiedErrorId : RequiredWindowsUpdateNotInstalled,Install-Package,Microsoft.PowerShell.PackageManagement

.Cmdlets.InstallPackage

Docker dla systemu Windows Server 2016 wymaga aktualizacji „KB3176936”. Można pobrać go z witryny Windows Update, a następnie zainstalować ręcznie:

http://www.catalog.update.microsoft.com/search.aspx?q=kb3176936



Lub można wykonać to zadanie za pomocą narzędzia sconfig, a następnie wybrać numer 6:

==========

==========

Server Configuration

==========
==========
=======

1) Domain/Workgroup: Domain: get-cmd.Local
2) Computer Name: SRV1
3) Add Local Administrator
4) Configure Remote Management Enabled

5) Windows Update Settings: DownloadOnly
6) Download and Install Updates
7) Remote Desktop: Enabled (more secure clients only)

8) Network Settings
9) Date and Time
10) Telemetry settings Basic
11) Windows Activation

12) Log Off User
13) Restart Server
14) Shut Down Server
15) Exit to Command Line

Windows pobierze i zainstaluje aktualizacje:

Microsoft (R) Windows Script Host Version 5.812

Copyright (C) Microsoft Corporation. All rights reserved.

Search for for (A)ll updates or (R)ecommended updates only? a

Searching for all applicable updates.

Downloading updates...

Drugi sposób polega na zainstalowaniu wersji rozwojowej Docker, aby mieć najnowsze funkcje. Należy pobrać Docker bezpośrednio z oficjalnej strony internetowej, a następnie użyć polecenia cmdlet Invoke-WebRequest:

PS > Invoke-WebRequest "https://master.dockerproject.org/windows/amd64/docker-1.14.0-dev.zip" -OutFile "$env:TEMP\docker.zip" –UseBasicParsing

Dalej należy wyodrębnić archiwum za pomocą komendy Expand-Archive:

PS > Expand-Archive -Path "$env:TEMP\docker.zip" -DestinationPath $env:ProgramFiles

Teraz można utworzyć zmienną środowiskową:

PS > $env:path += ";$env:ProgramFiles\Docker"

PS > $existingMachinePath = [Environment]::GetEnvironmentVariable("Path",

[System.EnvironmentVariableTarget]::Machine)

PS > [Environment]::SetEnvironmentVariable("Path", $existingMachinePath + ";$env:ProgramFiles\Docker", [EnvironmentVariableTarget]::Machine)

Aby zakończyć, należy zainstalować Docker jako usługę Windows. Należy uruchomić następujące polecenie, aby zarejestrować plik dockerd.exe:

PS > dockerd --register-service

Po zainstalowaniu usługa może zostać uruchomiona:

PS > Start-Service Docker

WARNING: Waiting for service 'Docker Engine (Docker)' to start...

PS > Get-Service -name "docker*"

Status	Name	DisplayName
Running	docker	Docker Engine

Aby wyświetlić informacje o Dockerze, należy uruchomić następujące opcje:

```
PS C:\> docker info
Containers: 0
 Running: 0
 Paused: 0
 Stopped: 0
Images: 0
```

Server Version: 1.14.0-dev

Storage Driver: windowsfilter

Windows:

Logging Driver: json-file

Plugins:

Volume: local

Network: l2bridge l2tunnel nat null overlay transparent

Swarm: inactive

Default Isolation: process

Kernel Version: 10.0 14393 (14393.0.amd64fre.rs1_release.160715-1616)

Operating System: Windows Server 2016 Datacenter

OSType: windows

Architecture: x86_64

CPUs: 1

Total Memory: 1.933 GiB

Name: SRV1

ID: VB3B:IGYN:GEFL:6ML7:OQJM:GMCJ:HDNU:Z57W:SWYI:Z2I3:WZKG:O2L4

Docker Root Dir: C:\ProgramData\docker

Debug Mode (client): false

Debug Mode (server): false

Registry: https://index.docker.io/v1/

Experimental: false

Insecure Registries:

127.0.0.0/8

Live Restore Enabled: false

Ok, teraz host kontenera działa, więc można wdrożyć nasz pierwszy kontener Windows! W pierwszym przykładzie wdrożymy kontener IIS, uruchamiając następujące polecenie:

```
PS > Docker run -d -p 8080:80 --name iis microsoft/iis
Unable to find image 'microsoft/iis:latest' locally
latest: Pulling from microsoft/iis
c480435b7cba: Downloading [==>
          ] 220.1 MB/4.175 GB
2acd7c473906: Downloading [==============>
                    ] 240.1 MB/922.1 MB
a837699b27ea: Download complete
e4e8167eafc5: Download complete
0344b06e0e62: Download complete
```

Poniżej znajduje się składnia polecenia Docker:

```
PS > docker run PUBLIC_PORT:PRIVATE_CONTAINER_PORT CONTAINER_NAME IMAGE
```

Kontenery wykorzystują koncepcję PAT (tłumaczenie adresu portu). Oznacza to, że konieczne jest porty

ujawnienie portów kontenera przez hosta kontenera. W naszym przykładzie Docker zwiąże kontener numer portu 80 z numerem hosta kontenera portu 8080. Następnie, gdy spróbujemy otworzyć stronę IIS znajdującą się wewnątrz kontenera, należy użyć publicznego portu 8080.

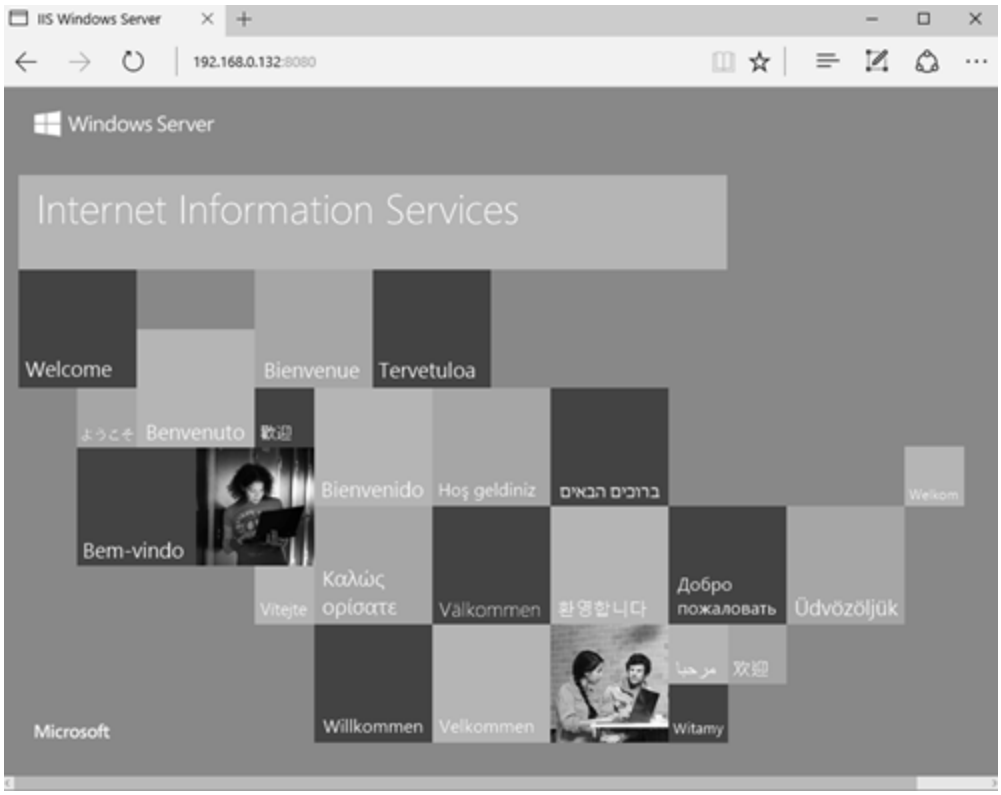
Parametr «Nazwa» dodaje przyjazną nazwę do kontenera. Nie jest to obowiązkowe, ale może się przydać później zarządzanie pojemnikami.

Na koniec należy podać nazwę obrazu pojemnika. Tutaj trzeba wybrać obraz IIS dostarczony przez Microsoft.

Po uruchomieniu polecenia system Windows sprawdza, czy obraz jest dostępny lokalnie (na hoście kontenera). Jeśli nie, wówczas Docker pobiera obraz z koncentratora Docker.

```
PS > Docker run -d -p 8080:80 --name iis microsoft/iis
Unable to find image 'microsoft/iis:latest' locally
…
```

Kiedy to zrobimy, nasz kontener Windows będzie działał. Nasz host kontenera ma następujący adres IP: 192.168.0.132, więc nasza witryna IIS jest dostępna od 192.168.0.132:8080.



51.2. Image2Docker

Powiedzmy, że mamy serwer, który został pieczołowicie wykonany ręcznie i chcemy go konteneryzować? Można użyć modułu PowerShell „Image2Docker” dostępnego w witrynie GitHub: https://github.com/docker/communitytools-image2docker-win, która przenosi istniejące obciążenia aplikacji Windows z maszyn wirtualnych na obrazy Docker. Można więc łatwo przekonwertować usługi Windows na Windows Containers, takie jak: witryny IIS, DNS, DHCP.

Licencjonowanie

Oficjalna witryna zawiera stosunkowo mało informacji na temat licencjonowania, ale zgodnie z arkuszem licencyjnym Windows Server 2016, Standard Edition zapewnia prawa do maksymalnie 2 kontenerów Hyper-V, gdy wszystkie fizyczne rdzenie na serwerze są licencjonowane i nieograniczone kontenery Windows Server dla obu wersji.

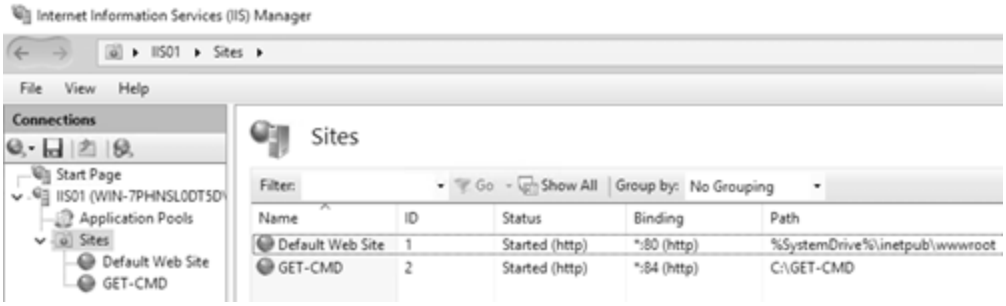
Windows Server 2016 Editions		
	Datacenter Edition	Standard Edition
Core functionality of Windows Server	●	●
OSEs/Hyper-V containers*	Unlimited	2
Windows Server containers	Unlimited	Unlimited

Jak to działa?

Image2Docker najpierw sprawdza artefakty w obrazie VM systemu Windows Server 2003, 2008, 2012 lub 2016 –

w formacie WIM, VHD lub VHDX. Następnie wyodrębnia całą maszynę wirtualną lub określone artefakty z pliku VHD. Następnie wygeneruje plik Docker, który można wbudować w obraz Docker. Ten moduł PowerShell wymaga PowerShell 5.0 lub nowszego.

Opiszę teraz kroki niezbędne do wyodrębnienia artefaktów IIS. Na poniższym zrzucie ekranu zainstalowałem maszynę wirtualną Windows Server 2016 z zainstalowaną rolą IIS o nazwie „IIS01”. Ta maszyna wirtualna ma dwie witryny IIS:



Najpierw należy zainstalować moduł PowerShell Image2Docker na hoście kontenera:

```
PS > Install-Module Image2Docker
    Untrusted repository
     You are installing the modules from an untrusted repository. If you trust this repository, change its
    InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
    'PSGallery'?
    [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): Y
```

Następnie można użyć polecenia ConvertTo-DockerFile. To polecenie przeskanuje obraz źródłowy (np. Plik VHDX lub WIM), aby określić artefakt. Image2Docker obsługuje obecnie wykrywanie następujących artefaktów:

```
PS > Get-WindowsArtifact
  AddRemovePrograms
  AllWindowsFeatures
  Apache
  DHCPServer
  DNSServer
  IIS
  MSMQ
  SQLServer
```

Aby zeskanować obraz, wystarczy wywołać polecenie ConvertTo-Dockerfile i określić parametr – ImagePath, zawierający plik VHDX. Folder wyjściowy będzie zawierał wygenerowany plik docker. Przed skanowaniem obrazu należy wyłączyć maszynę wirtualną.

```
PS > Import-Module Image2Docker
    PS > ConvertTo-Dockerfile -ImagePath "C:\Hyper-V\IIS01\Virtual Hard Disks\IISV01.vhdx" -OutputPath "C:\Containers" -Artifact IIS -Verbose
```

VERBOSE: Reading image file: C:\Hyper-V\IIS01\Virtual Hard Disks\IIS01.vhdx

VERBOSE: Image file appears to be a valid WIM or VHDX file.

VERBOSE: Image file C:\Hyper-V\IIS01\Virtual Hard Disks\IIS01.vhdx contains 1 images

VERBOSE: This image appears to be a valid Virtual Hard Drive (VHDX) file.

VERBOSE: Image type is: VHDX

VERBOSE: User didn't specify a mount path. Using:

C:\Users\Nicolas\AppData\Local\Temp\94decd22-a9aa-45d7-9402-a309c2fa39b0-mount

VERBOSE: Finished mounting image C:\Hyper-V\IIS01\Virtual Hard Disks\IIS01.vhdx at mount point

C:\Users\Nicolas\AppData\Local\Temp\94decd22-a9aa-45d7-9402-a309c2fa39b0-mount

VERBOSE: Finished mounting image to: C:\Users\Nicolas\AppData\Local\Temp\94decd22-a9aa-45d7-9402-a309c2fa39b0-mount

VERBOSE: Starting conversion process

VERBOSE: Started discovering IIS artifact

VERBOSE: Checking IIS ApplicationHost config for Windows Version: 10.0

VERBOSE: Target Image Version 10.0.14393.0

VERBOSE: IIS service is present on the system

VERBOSE: ASP.NET is NOT present on the system

VERBOSE: .NET 3.5 is NOT present on the system

VERBOSE: Finished discovering IIS artifact

VERBOSE: Generating Dockerfile based on discovered artifacts in

:C:\Users\Nicolas\AppData\Local\Temp\94decd22-a9aa-45d7-9402-a309c2fa39b0-mount

VERBOSE: Generating result for IIS component

VERBOSE: Copying IIS configuration files

VERBOSE: Writing instruction to create site Default Web Site

VERBOSE: Processing source directory: C:\inetpub\wwwroot

VERBOSE: Writing instruction to expose port for site Default Web Site

VERBOSE: Writing instruction to create site GET-CMD

VERBOSE: Processing source directory: C:\GET-CMD

VERBOSE: Writing instruction to expose port for site GET-CMD

VERBOSE: Finished generating the Dockerfile

VERBOSE: Finished dismounting the Windows image from

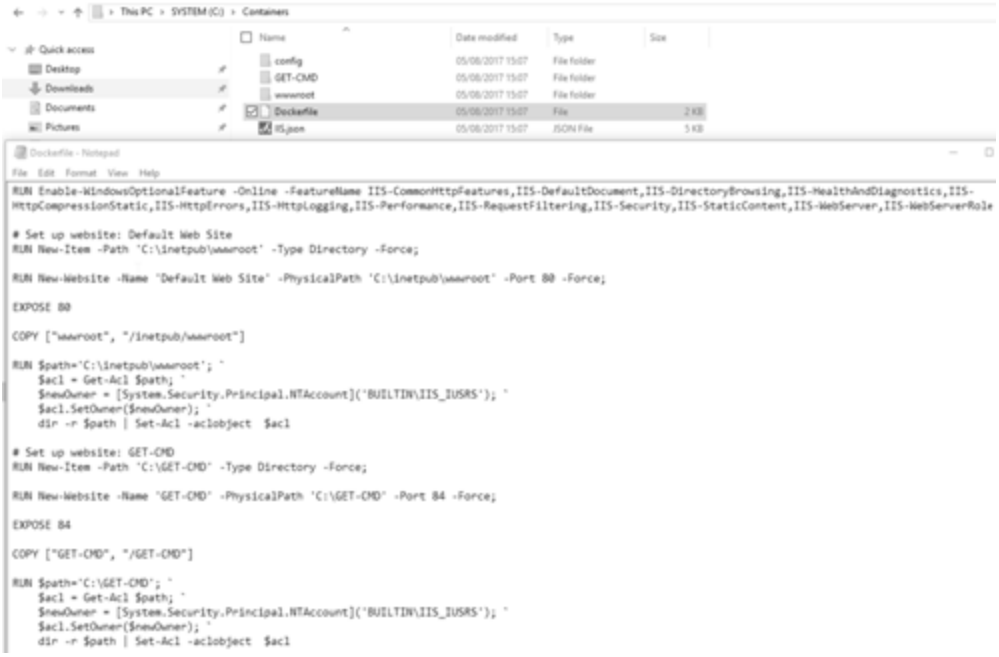
C:\Users\Nicolas\AppData\Local\Temp\94decd22-a9aa-45d7-9402-a309c2fa39b0-mount

Można również wyodrębnić pojedynczą witrynę z maszyny wirtualnej IIS przy użyciu parametru –ArtifactParam,

a następnie nazwy witryny IIS:

PS > ConvertTo-Dockerfile -ImagePath "C:\Hyper-V\IIS01\Virtual Hard Disks\IIS01.vhdx" -OutputPath "C:\Containers" -Artifact IIS -ArtifactParam "GET-CMD" –Verbose

Teraz można przejść do folderu wyjściowego, a zauważysz będzie można zauważyć, że został utworzony plik Docker.

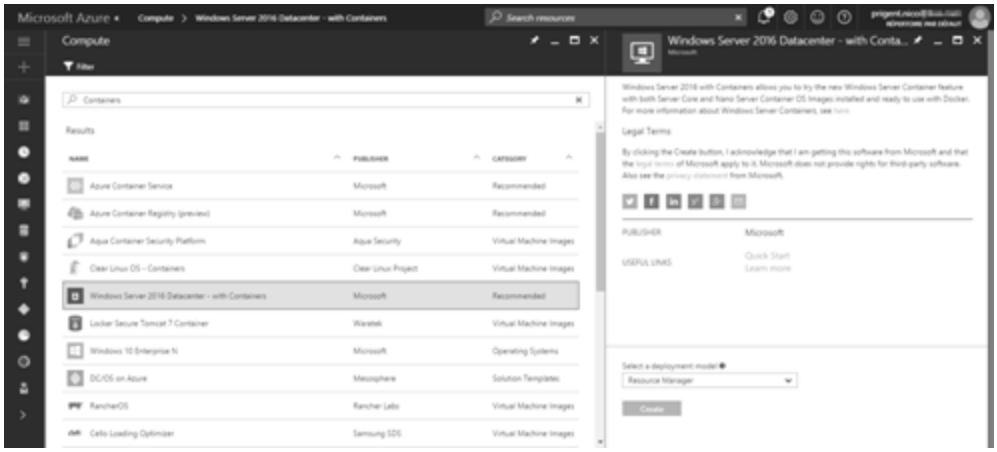


Jeśli mamy tylko plik VMDK, można użyć narzędzia Microsoft Virtual Machine Converter do konwersji obrazów VMDK na obrazy VHD.

51.3. Windows Server 2016 z kontenerami na platformie Azure

Dla wielu programistów i sysadminów rozsądnie jest wdrażać usługi w chmurze Microsoft Azure, ale mamy dodatkową opcję wdrożenia hosta kontenera do chmury Microsoft Azure. Jedną z zalet używania Azure w ten sposób jest możliwość wdrożenia maszyny wirtualnej Windows Server 2016 z już zainstalowaną funkcją Kontenery. W ten sposób można eksperymentować z kontenerem Windows Server, z zainstalowanymi obrazami Server Core i Nano Server Container OS i gotowymi do użycia z Dockerem.

Należy się zalogować do portalu Azure i utworzyć maszynę wirtualną za pomocą obrazu Windows Core 2016 z kontenerami, jak pokazano poniżej:



51.4. Komendy Dockera

Jak ustawić pracę z Dockerem na Windows Server? Zanim przejdziemy do praktycznej strony, należy zapoznać się

z podstawowymi poleceniami Docker PowerShell. Można uruchomić polecenie docker-help:

Commands:

attach Attach to a running container
build Build an image from a Dockerfile
commit Create a new image from a container's changes
cp Copy files/folders between a container and the local filesystem
create Create a new container
diff Inspect changes on a container's filesystem
events Get real time events from the server
exec Run a command in a running container
export Export a container's filesystem as a tar archive
history Show the history of an image
images List images
import Import the contents from a tarball to create a filesystem image
info Display system-wide information
inspect Return low-level information on a container, image or task
kill Kill one or more running containers
load Load an image from a tar archive or STDIN

login Log in to a Docker registry.

logout Log out from a Docker registry.

logs Fetch the logs of a container

pause Pause all processes within one or more containers

port List port mappings or a specific mapping for the container

ps List containers

pull Pull an image or a repository from a registry

push Push an image or a repository to a registry

rename Rename a container

restart Restart one or more containers

rm Remove one or more containers

rmi Remove one or more images

run Run a command in a new container

save Save one or more images to a tar archive (streamed to STDOUT by default)

search Search the Docker Hub for images

start Start one or more stopped containers

stats Display a live stream of container(s) resource usage statistics

stop Stop one or more running containers

tag Tag an image into a repository

top Display the running processes of a container

unpause Unpause all processes within one or more containers

update Update configuration of one or more containers

version Show the Docker version information

wait Block until one or more containers stop, then print their exit codes

Run 'docker COMMAND --help' for more information on a command.

Tyle komend wystarczy do codziennego użytku. Należy zacząć od użycia jednego z najpopularniejszych poleceń Docker:

PS > docker images

To polecenie pokazuje, które obrazy Docker są dostępne lokalnie. Po zainstalowaniu Windows Containers nie zainstalowano jeszcze żadnych obrazów Docker. Pierwszą rzeczą, którą należy zrobić, to pobrać obrazy Windows Server z Docker Hub. Aby wykonać to zadanie, nie potrzeba konta Docker Hub:

PS > docker pull <image_name>

Opiszę to polecenie bardziej szczegółowo w następnej sekcji. Jeśli mamy co najmniej jeden dostępny obraz, można uruchomić Kontener Windows:

PS > docker run ––name <Container_Name> <Image_Name>

Oznacza to, że Kontener Windows nazwany <Container_Name> zostanie uruchomiony z obrazu o nazwie <Image_Name>. Jeśli mamy więcej niż jeden

kontener, może być przydatne uzyskanie listy wszystkich uruchomionych kontenerów:

```
PS > docker ps
```

Na koniec będziemy potrzebować informacji o swoich kontenerach, takich jak adres IP. Należy użyć następujących informacji, aby pobrać te informacje:

```
PS > docker inspect
```

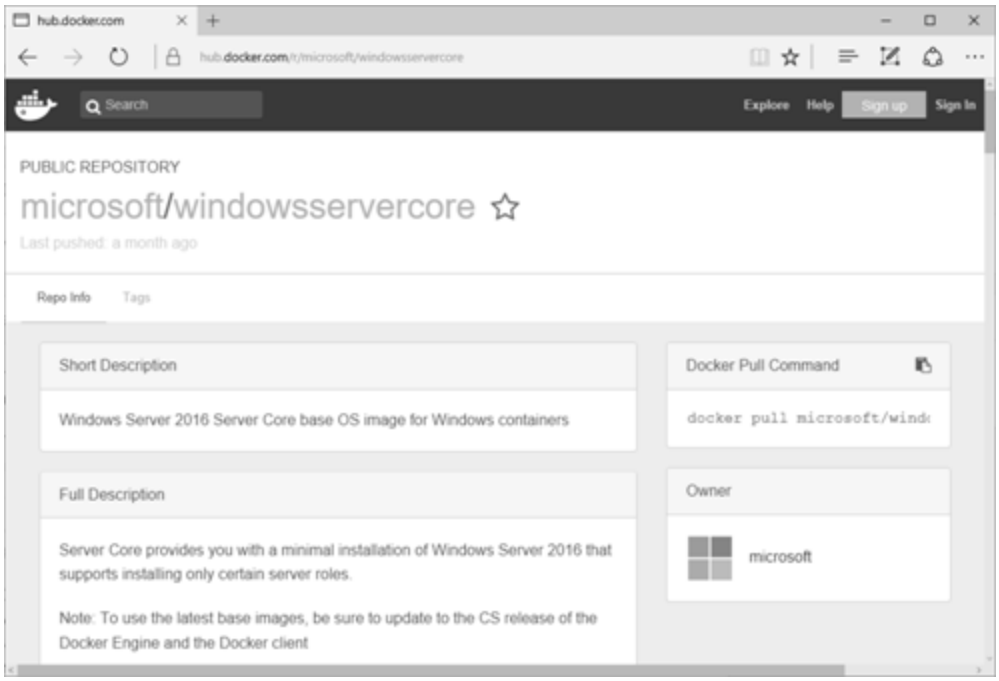
51.5. Retrieve Images from Docker Hub

W żargonie kontenerowym Dockera obraz jest szablonem, z którego odradzają się nowe kontenery. Możemy pobrać kilka gotowych obrazów Docker z Docker Hub. W momencie, w którym zostało to napisane, firma Microsoft ma dwa obrazy kontenerów w swojej galerii: Nano Server i Windows Server Core. Pobierzmy je, pobierając obrazy z Docker Hub:

```
PS > docker images
  REPOSITORY          TAG                 IMAGE ID
CREATED             SIZE
  PS > docker pull microsoft/windowsservercore
  Using default tag: latest
  latest: Pulling from microsoft/windowsservercore
```

```
3889bb8d808b: Downloading [=>
                ] 102.7 MB/4.07 GB
3430754e4d17: Downloading [=====>
                      ] 102.2 MB/913.1 MB
PS > docker pull microsoft/nanoserver
[…]
```

Ok, ale jak poznać dokładną nazwę obrazu, którego potrzebujemy? To całkiem proste. W Docker Hub można zauważyć następującą sekcję „Docker Pull Command”, jak pokazano poniżej.



Jedynym niezbędnym krokiem jest skopiowanie i wklejenie polecenia, aby pobrać obraz. Po zakończeniu procesu instalacji obrazu (może to chwilę potrwać, w zależności od szybkości połączenia internetowego), sprawdź należy sprawdzić, czy obraz Windows Server Core

jest dostępny lokalnie, a następnie uruchomić polecenie docker images, aby sprawdzić:

```
PS > docker images
 REPOSITORY                          TAG                 IMAGE ID
 CREATED             SIZE
  microsoft/windowsservercore        latest
4d83c32ad497        6 weeks ago         9.56GB
   microsoft/nanoserver               latest
d9bccb9d4cac        6 weeks ago         925MB
```

Jeśli wdrożono wstępnie skonfigurowaną maszynę wirtualną na platformie Azure, dwa podstawowe obrazy są już wyciągnięte.

51.6. Wdrażanie nowego kontenera Windows

Teraz należy użyć polecenia Docker run do wdrożenia nowego kontenera o nazwie CoreServerCMD, który wykorzystuje obraz Windows Server Core. Przełącznik –it oznacza sesję interaktywną, a cmd.exe oznacza, że chcemy wprowadzić kontener wewnątrz nowej konsoli cmd.exe. Należy uważać, gdyż nazwa repozytorium musi być pisana małymi literami.

```
PS > docker run -it --name CoreServerCMD microsoft/windowsservercore cmd.exe
```

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\>ipconfig
Windows IP Configuration
Ethernet adapter vEthernet (Container NIC b4dc9191):
   Connection-specific DNS Suffix  . :
         Link-local IPv6 Address . . . . . : fe80::81ac:61de:7cef:3467%17
   IPv4 Address. . . . . . . . . . . : 172.21.149.87
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.21.144.1
```

Teraz mamy uruchomiony kontener o nazwie CoreServerCMD. Można sprawdzić za pomocą polecenia docker ps:

```
PS > docker ps
 CONTAINER ID  IMAGE                          COMMAND
CREATED       STATUS       NAMES
 9e8e23686548  microsoft/windowsservercore "cmd.exe"
5 minutes ago Up 3 minutes CoreServerCMD
```

Polecenie docker ps domyślnie pokazuje tylko działające kontenery, ale przekazanie flagi -a do polecenia spowoduje wyświetlenie wszystkich kontenerów. Kontenery można uruchamiać i zatrzymywać w bardzo prosty sposób, uruchamiając:

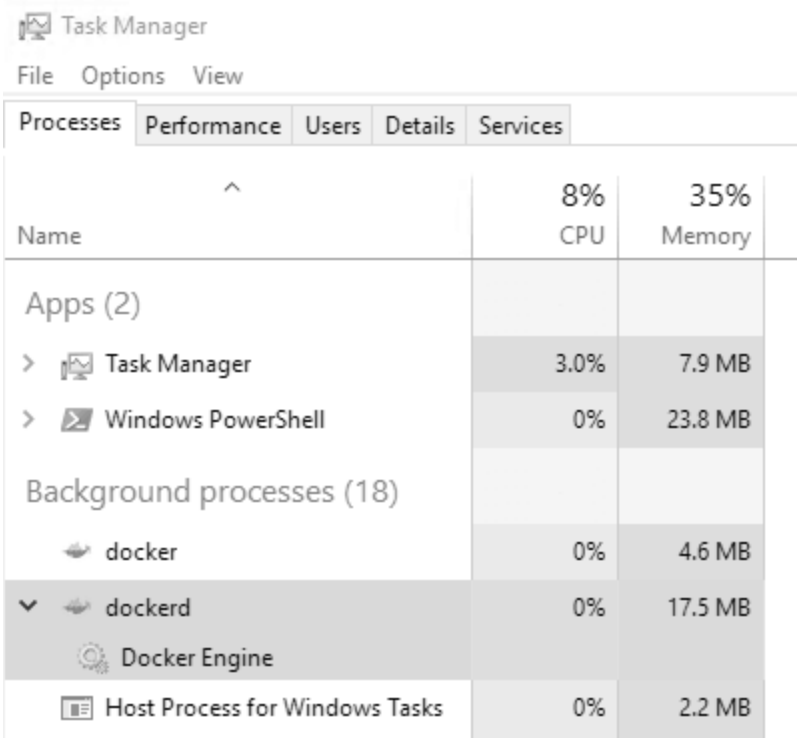
PS > docker stop CoreServerCMD

CoreServerCMD

PS > docker start CoreServerCMD

CoreServerCMD

Po uruchomieniu Windows Container, trzeba spojrzeć na narzędzie Task Manager, a można zauważyć nowy proces o nazwie „Docker”. Po zatrzymaniu kontenera proces ten zniknie:



OK, kontener jest uruchomiony, ale nie trzeba ponownie wykonywać polecenia docker run. Aby ponownie wejść do

uruchomionego kontenera, polecenie docker attach wykona zadanie:

PS > docker attach CoreServerCMD

Kontenery mają zarówno nazwę, jak i identyfikator, a każdy z nich może być użyty do identyfikacji kontenera do kontroli. Inspect to podstawowa instrukcja Dockera (Docker Docs- Docker Inspect), którya pozwala uzyskać wszystkie informacje o kontenerze i obrazie. Poniżej sprawdzimy nasz kontener:

```
PS > docker inspect CoreServerCMD
  [
     {
                                                    "Id":
"9e8e236865487f3f715d2b1d5582512d9f068f97219c01249
a497e03afcff94d",
          "Created": "2017-02-26T12:20:41.2866341Z",
          "Path": "cmd.exe",
          "Args": [],
          "State": {
             "Status": "exited",
             "Running": false,
             "Paused": false,
             "Restarting": false,
             "OOMKilled": false,
```

```
            "Dead": false,
            "Pid": 0,
            "ExitCode": 9009,
            "Error": "",
                                    "StartedAt":    "2017-02-
26T12:24:24.8655415Z",
                                   "FinishedAt":    "2017-02-
26T12:32:26.5074121Z"
        },
                                                    "Image":
"sha256:4d83c32ad497f063ae77377afb9285ed3f8a2d2dc52
eb53268a7152777b25add",
        "ResolvConfPath": "",
        "HostnamePath": "",
        "HostsPath": "",
                                                  "LogPath":
"C:\\ProgramData\\docker\\containers\\9e8e236865487f3f
715d2b1d5582512d9f068f97219c01249a497e03afcff94d\\9
e8e236865487f3f715d2b1d5582512d9f068f97219c01249a4
97e03afcff94d-json.log",
        "Name": "/CoreServerCMD",
        "RestartCount": 0,
        "Driver": "windowsfilter",
        "MountLabel": "",
        "ProcessLabel": "",
        "AppArmorProfile": "",
```

```
            "ExecIDs": null,
            "HostConfig": {
                "Binds": null,
                "ContainerIDFile": "",
                "LogConfig": {
                    "Type": "json-file",
                    "Config": {}
                },
                "NetworkMode": "default",
                "PortBindings": {},
                "RestartPolicy": {
                    "Name": "no",
                    "MaximumRetryCount": 0
    […]
```


Dane wyjściowe zostały obcięte. Można wyświetlić określone ustawienia, używając parametru -f:

```
PS > docker inspect -f '{{.Config.Hostname}}' CoreServerCMD
9e8e23686548
PS > docker inspect -f '{{.Config.Image}}' CoreServerCMD
microsoft/windowsservercore
PS > docker inspect -f '{{.NetworkSettings.IPAddress}}' CoreServerCMD
172.21.149.87
```

51.7. Budowanie własnego obrazu kontenera

Kontenery Docker są tworzone przy użyciu obrazów podstawowych. Zasadniczo obraz nie może zawierać niczego więcej niż podstawy systemu operacyjnego lub może zawierać pełen stos aplikacji gotowy do użycia. Zobaczmy więc przykład. Można mieć niestandardową witrynę internetową, którą chcemy wdrożyć w kontenerze Windows. Mamy dwa sposoby na wykonanie tej pracy. Można uruchomić Windows Container lub po prostu użyć pliku Docker. Aby uruchomić kontener Windows, należy zainstalować i skonfigurować rolę IIS, a następnie zaimportować pliki HTML. Aby użyć pliku Docker, trzeba trochę wyjaśnić. Należy sobie wyobrazić, dla przykładu, że mamy folder o nazwie „MyWebSite” zawierający dwa pliki:

- Index.html,
- Dockerfile.

Czym jest Dockerfile?

Dockerfile to skrypt składający się z różnych „poleceń” zwanych również „instrukcjami” i argumentów wymienionych automatycznie w celu automatycznego wykonywania akcji na obrazie podstawowym w celu utworzenia nowego. Plik Dockerfile znacznie ułatwia wdrażanie, automatyzując i upraszczając ten proces.

Poniżej znajduje się zawartość naszego pliku Dockerfile:

FROM microsoft/iis

```
MAINTAINER Nicolas PRIGENT
RUN mkdir C:\site
RUN powershell -NoProfile -Command \
  Import-module IISAdministration; \
    New-IISSite -Name "Site" -PhysicalPath C:\site -BindingInformation "*:8080:"
COPY index.html C:\site
EXPOSE 8080
```

Nasz plik Dockerfile zaczyna się od słowa kluczowego „FROM”. To słowo kluczowe definiuje obraz, z którego rozpoczyna się proces kompilacji. W naszym przykładzie użyjemy obrazu Microsoft IIS, następnie utworzymy folder i na końcu uruchomimy niektóre polecenia PowerShell za pomocą słowa kluczowego „RUN”. Dzięki temu Dockerfile, Docker utworzy nowy obraz kontenera. Obraz kontenera to przechwycona informacja o stanie kontenera, który został utworzony i dostosowany na hoście kontenerowym. Po dostosowaniu obrazu kontenera do określonego celu, można go użyć do utworzenia z niego nowych kontenerów. Jest to coś w rodzaju „Szablonu” do tworzenia nowych kontenerów do określonego celu, który można wyświetlić za pomocą polecenia docker images.

51.8. Tworzenie obrazu kontenera

OK, nasz plik Dockerfile jest gotowy. Oto polecenia, które należy uruchomić, aby utworzyć nowy obraz:

```
PS > cd C:\MyWebsite
  PS C:\MyWebsite> docker build -t myiis .
  Sending build context to Docker daemon  3.072kB
  Step 1/6 : FROM microsoft/iis
   ---> a3dd2dff392b
  Step 2/6 : MAINTAINER Nicolas PRIGENT
   ---> Running in 2325e0d1cad2
   ---> 5c647612617c
  Removing intermediate container 2325e0d1cad2
  Step 3/6 : RUN mkdir C:\site
   ---> Running in bec661fdb10c
   ---> 5173bcee6d03
  Removing intermediate container bec661fdb10c
  Step 4/6 : RUN powershell -NoProfile -Command Import-module IISAdministration; New-IISSite -Name "Site" -PhysicalPath C:\site -BindingInformation "*:8080:"
   ---> Running in d9abe719e201
   ---> 0d84ea9a9af5
  Removing intermediate container d9abe719e201
  Step 5/6 : COPY index.html C:\site
   ---> b6b3342f2761
  Removing intermediate container 45e11d3a432f
  Step 6/6 : EXPOSE 8080
   ---> Running in 7f8983d773d5
```

```
 ---> f815a0ab0695
Removing intermediate container 7f8983d773d5
Successfully built f815a0ab0695
```

„myiis” to nazwa repozytorium i musi być pisana małymi literami. Pod koniec naszego Dockerfile pokazuję moją stronę internetową na porcie 8080. Na tym etapie można potwierdzić, że nasz obraz kontenera został pomyślnie utworzony:

```
PS > docker images
REPOSITORY                          TAG                 IMAGE ID
CREATED             SIZE
myiis                               latest              5b4148e14c8f
45 seconds ago      9.82GB
microsoft/iis                       latest              a3dd2dff392b
6 weeks ago         9.82GB
microsoft/windowsservercore         latest
4d83c32ad497        7 weeks ago         9.56GB
microsoft/nanoserver                latest
d9bccb9d4cac        7 weeks ago         925MB
```

Teraz po prostu należy użyć polecenia docker run, aby utworzyć nowy kontener z naszego nowego obrazu kontenera:

PS > docker run -d -p 8080:8080 --name websitecontainer myiis

PS > docker ps

CONTAINER ID IMAGE […] STATUS PORTS NAMES

a6a41cf3b19c myiis […] Up Less than a second 0.0.0.0:8080->8080/tcp websitecontainer

Nasz kontener działa. Można uzyskać adres IP kontenera za pomocą następującego polecenia i przejść do witryny pod następującym adresem URL: http://172.21.158.179:8080.

PS > docker inspect -f '{{range .NetworkSettings.Networks}}{{.IPAddress}}{{end}}' a6a41cf3b19c

172.21.158.179

Or

PS > docker inspect -f '{{range .NetworkSettings.Networks}}{{.IPAddress}}{{end}}' websitecontainer

172.21.158.179

bądź należy być ostrożnym, ponieważ, jeśli zaczniemy od Docker i Windows Containers, prawdopodobne jest błąd popełnienie błędu: próba uzyskania adres IP z obrazu zamiast z kontenera. Należy się upewnić, że otrzymaliśmy identyfikator kontenera z docker ps. Jeśli używamy nazwy obrazu, należy zapytać Dockera, aby pokazał adres IP

obrazu. To oczywiście nie ma sensu, ponieważ obrazy nie mają adresów IP.

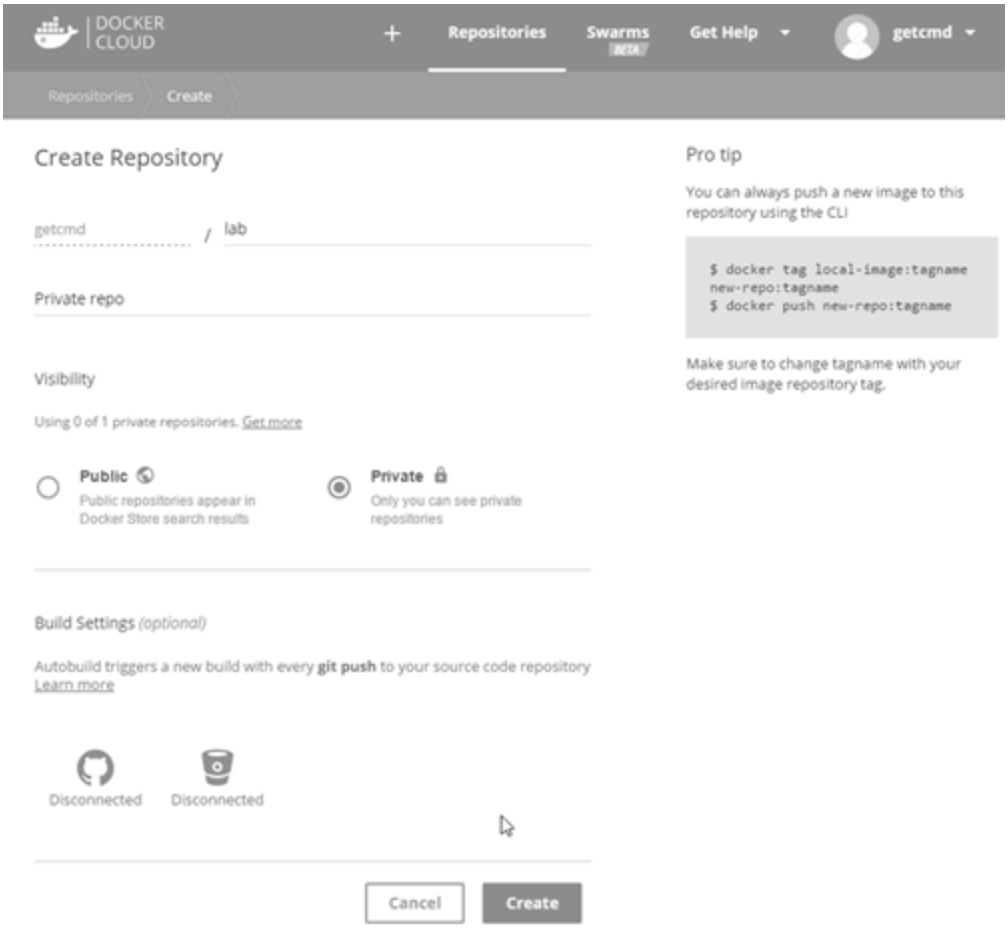
51.9. Przesyłanie obrazu do Docker Hub

Najpierw należy utworzyć bezpłatne konto Docker tutaj: https://cloud.docker.com/. Docker Hub pozwala przechowywać i udostępniać swoje podstawowe obrazy. Oznacza to, że współpracownicy mogą używać naszego podstawowego obrazu z naszego repozytorium.

Można tworzyć repozytoria i ręcznie przesuwać obrazy za pomocą polecenia docker push. Te repozytoria mogą być publiczne lub prywatne. Można utworzyć prywatne

repozytorium za darmo i nieograniczoną liczbę publicznych repozytoriów.

Należy kliknąć Repositories i Create. Teraz trzeba podać nazwę i opcjonalny opis. Następnie należy wybrać ustawienie widoczności dla repozytorium.



Kiedy potrzebujemy przesłać obraz do Docker Hub, należy użyć trzech poleceń, pierwsze:

PS > docker tag f45ecff4c38c getcmd/lab:latest

- Getcmd to mój Docker ID.
- Lab to moje prywatne repozytorium.

- Latest to Tag.

Należy uruchomić teraz komendę docker images, aby zweryfikować, czy istnieje ten sam ID obrazu w dwóch osobnych repozytoriach.

```
PS > docker images
  REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
  getcmd/lab          latest              f45ecff4c38c        2 hours ago         9.89GB
  myiis               latest              f45ecff4c38c        2 hours ago         9.89GB
```

Drugie polecenie przechowuje nasze poświadczenia za pomocą polecenia docker login:

```
PS > docker login

  Login with your Docker ID to push and pull images from Docker Hub. If you don't have a Docker ID, head over to https://hub.docker.com to create one.

  Username: getcmd
  Password:
  Login Succeeded
```

Teraz można przesłać obraz:

```
PS > docker push getcmd/lab
```

The push refers to a repository [docker.io/getcmd/lab]

0a2abd09b43e: Pushed

68da241f1f36: Pushed

26de02533429: Pushed

12af8be2d3dc: Pushed

b54f48930406: Pushed

5b4aace84103: Mounted from microsoft/iis

1f2f3eb32edc: Pushed

0451551dda21: Pushed

c28d44287ce5: Skipped foreign layer

f358be10862c: Skipped foreign layer

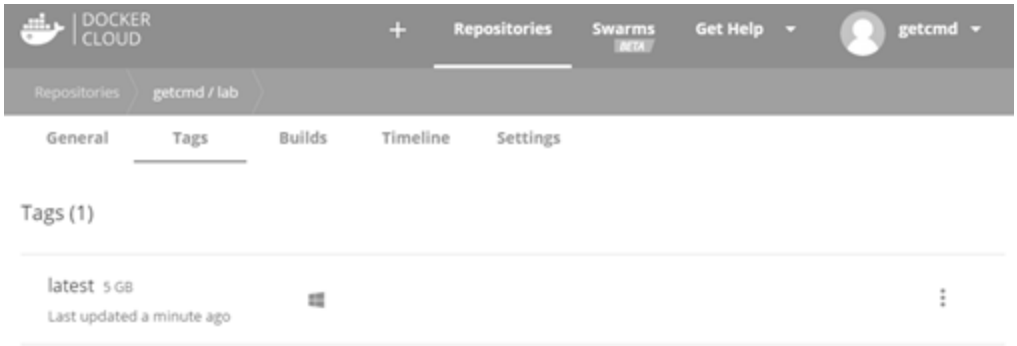
latest:

digest:

sha256:95fa14a4e1af0d8b52ed6dc10c06b6f1085285126ddef2882210dd904de88565

size: 2619

latest: digest: size: 2619



Uwaga: Można wylogować się z Docker Hub przy użyciu polecenia docker logout.

Teraz trzeba zrozumieć różnice między kontenerami Linux, kontenerami Windows Server i kontenerami Hyper-V. Można wtedy definiować, tworzyć i uruchamiać wieloskładnikowe aplikacje Docker i przenosić istniejące maszyny wirtualne Windows Container do Docker.

51.10. Kontenery Linux w systemie Windows: niwelowanie różnic

Zanim przejdziemy dalej, muszę zademonstrować, że jeśli spróbujemy uruchomić kontener Linux na moim hoście kontenerowym Windows, próba zakończy się niepowodzeniem, ponieważ jądra systemu Windows i Linux są zasadniczo różne. Obecnie nie można uruchamiać kontenerów opartych na systemie Linux na hoście kontenerów systemu Windows:

```
PS > docker pull wordpress
  Using default tag: latest
  latest: Pulling from library/wordpress
  image operating system "linux" cannot be used on this platform
```

Ten problem został rozwiązany, a programiści wkrótce będą mogli uruchamiać kontenery Linux natywnie na serwerze Windows Server, używając technologii izolacji kontenera Hyper-V. Microsoft ogłosił ten fakt podczas

konferencji DockerCon 2017, odbywającej się w Austin w Teksasie. Kiedy to zostanie wydane, usunie to potrzebę oddzielnych infrastruktur i narzędzi programistycznych dla obu systemów operacyjnych. Podczas tego samego wydarzenia DockerCon zespół The Docker ogłosił LinuxKit, bezpieczny i przenośny podsystem Linux dla ruchu kontenerów. LinuxKit zapewni narzędzia, które pozwolą nam budować niestandardowe podsystemy Linux, które zawierają tylko komponenty wymagane przez platformę uruchomieniową. Projekt dotyczący tej nowej możliwości został oficjalnie rozpoczęty podczas wydarzenia. Docker będzie współpracować z firmą Microsoft w celu zintegrowania podsystemu LinuxKit z izolacją Hyper-V.Docker-Compose.

51.11. Izolacja Hyper-V

Podczas pracy w systemie Windows 10 można pracować tylko z kontenerami Hyper-V, ale podczas korzystania z systemu Windows Server 2016 można wybierać między kontenerami Hyper-V i Windows Server. Domyślnie, gdy użyjesz polecenia dokowania, uruchomisz kontener Windows Server, ale możesz określić, że chcesz uruchomić kontener Hyper-V za pomocą parametru -isolation = hyperv.

Przed uruchomieniem kontenera Hyper-V należy zainstalować rolę Hyper-V na hoście kontenera:

PS > Install-WindowsFeature -Name Hyper-V

Po uruchomieniu poprzedniego polecenia prawdopodobnie otrzymamy następujący komunikat o błędzie, jeśli nasz host kontenera jest maszyną wirtualną:

Hyper-V cannot be installed: The processor does not have required virtualization capabilities

Oznacza to, że zagnieżdżona wirtualizacja nie jest włączona w systemie. Wirtualizacja zagnieżdżona umożliwia uruchamianie hiperwizora wewnątrz maszyny wirtualnej działającej w środowisku Hypervisor. Aby włączyć wirtualizację zagnieżdżoną w Hyper-V, należy najpierw wyłączyć maszynę wirtualną Container Host, a następnie uruchomić następującą komendę PowerShell:

PS > Set-VMProcessor -VMName "VMName" -ExposeVirtualizationExtensions $true

Ta funkcja jest obecnie dostępna tylko dla Intela: wymagana jest Intel VT-x. Po zainstalowaniu roli Hyper-V można uruchomić swój pierwszy kontener Hyper-V, używając następującego skryptu na hoście kontenera:

PS > docker run --rm -it --name MyNanoHYPV --isolation=hyperv microsoft/nanoserver:latest

W tym przykładzie wdrażamy kontener Hyper-V o nazwie „MyNanoHYPV” z parametrem -isolation = hyperv, który jest oparty na obrazie Nano Server firmy Microsoft.

Microsoft Windows [Version 10.0.14393]

(c) 2016 Microsoft Corporation. All rights reserved.

```
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
   Connection-specific DNS Suffix  . :
                Link-local IPv6 Address . . . . . :
fe80::2890:b928:39d6:c8a%4
   IPv4 Address. . . . . . . . . . . : 172.21.158.25
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.21.144.1

C:\>hostname
b97558fd884a
```

Jak widać, kontener Hyper-V uruchamia się w kilka sekund; znacznie szybciej niż maszyna wirtualna. Aby potwierdzić, że korzystamy z kontenera Hyper-V, można przeprowadzić bardzo prostą kontrolę. Należy otworzyć konsolę PowerShell i użyć polecenia cmdlet Get-process, aby wyświetlić proces o nazwie "VMWP", który odpowiada procesowi Hyper-V:

```
PS > Get-Process -Name vmwp
 Handles NPM(K) PM(K) WS(K) CPU(s) Id SI
ProcessName
 ------- ------ ----- ----- ------ -- -- ----------
-
    3386 18 38796 20048 4.39 3632 0
vmwp
```

235 14 35888 16128 2.63 5224 0 vmwp

Z tego wyniku widać, że na hoście kontenera działają dwa procesy. Teraz po prostu należy wpisać polecenie „exit” wewnątrz kontenera Hyper-V i ponownie uruchomić poprzednie polecenie:

```
PS C:\Users\Administrator> Get-Process -Name vmwp

 Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName

 ------- ------ ----- ----- ------ -- -- -----------

 235 14 35888 16128 2.63 5224 0 vmwp

 PS C:\Users\Administrator>
```

Jest tylko jeden proces. Dlaczego? Kontener Hyper-V jest w pewnym sensie podobny do maszyny wirtualnej, ale inny jednak różni się od niej. Po uruchomieniu kontenera Hyper-V system Windows utworzy maszynę wirtualną, która w rzeczywistości nie jest maszyną wirtualną, ale jest pojemnikiem Hyper-V! Oczywiście nie widać tej maszyny wirtualnej w menedżerze konsoli Hyper-V. Jedyne, co można zobaczyć, to proces. Wykorzystanie kontenera Hyper-V zapewnia izolację trybu jądra zamiast izolacji trybu użytkownika.

Ok, teraz można przejrzeć inny przykład, aby zrozumieć różnicę między kontenerami Windows Server a kontenerami Hyper-V. Należy uruchomić następujące polecenie:

PS > docker run -d --name NanoWithoutHYPV microsoft/nanoserver:latest ping localhost –t

To polecenie wdraża kontener Windows Server oparty na obrazie Nano Server. Prowadzimy stałe pingowanie wewnątrz kontenera. Teraz należy użyć polecenia Docker Top, aby wyświetlić listę procesów uruchomionych w tym kontenerze:

PS > docker top NanoWithoutHYPV

Name	PID	CPU	Private Working Set
smss.exe	5384	00:00:00.140	208.9kB
csrss.exe	1920	00:00:00.437	356.4kB
wininit.exe	3320	00:00:00.031	651.3kB
services.exe	5780	00:00:00.203	1.487MB
lsass.exe	5752	00:00:00.234	1.95MB
svchost.exe	2800	00:00:00.062	1.241MB
svchost.exe	2856	00:00:00.031	1.323MB
svchost.exe	5852	00:00:00.125	2.179MB

```
  svchost.exe          5800                00:00:00.000
1.434MB
    svchost.exe        4544                00:00:00.140
3.752MB
    svchost.exe        4412                00:00:00.156
1.942MB
    svchost.exe        4844                00:00:00.062
1.47MB
    svchost.exe        5876                00:00:00.328
4.039MB
    svchost.exe        3016                00:00:00.109
2.327MB
    CExecSvc.exe       3136                00:00:00.000
737.3kB
    PING.EXE           3912                00:00:00.000
536.6kB
    PS C:\Users\Administrator> get-process *PING*
    Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI
ProcessName
    -------  ------    -----      -----     ------     --  --
-----------
         62       5      720       3480       0.00   3912   3
PING
```

Można zobaczyć, że ostatni proces, nazwany „PING.EXE”, odpowiada poleceniu ping wewnątrz kontenera. Ale uruchamiając polecenie Get-Process na hoście kontenera, zauważ można zauważyć, że ten sam proces istnieje z tym samym PID! Oznacza to, że nasz kontener Windows Server

używa zasobów Kernela z naszego hosta kontenera. OK, teraz należy zatrzymać ten kontener za pomocą polecenia Docker Stop i wykonać to samo, dodając parametr -isolation = hyperv:

PS > docker run -d --name NanoWithHYPV --isolation=hyperv microsoft/nanoserver:latest ping localhost –t

I uruchomić komendę Docker Top:

PS > docker top NanoWithHYPV

Name	PID	CPU	Private Working Set
smss.exe	828	00:00:00.312	213kB
csrss.exe	848	00:00:00.703	356.4kB
wininit.exe	888	00:00:00.140	618.5kB
services.exe	900	00:00:00.453	1.384MB
lsass.exe	916	00:00:00.406	1.933MB
svchost.exe	1008	00:00:00.109	1.237MB
svchost.exe	216	00:00:00.125	1.245MB
svchost.exe	444	00:00:00.187	1.184MB

svchost.exe 724 00:00:00.062 1.073MB

svchost.exe 984 00:00:00.375 3.895MB

svchost.exe 712 00:00:00.265 1.88MB

svchost.exe 1028 00:00:00.078 1.528MB

svchost.exe 1056 00:00:00.296 3.441MB

svchost.exe 1168 00:00:00.390 2.273MB

CExecSvc.exe 1188 00:00:00.031 737.3kB

PING.EXE 1396 00:00:00.046 532.5kB

PS C:\Users\Administrator> get-process *PING*

get-process : Cannot find a process with the name "ping". Verify the process name and call the cmdlet again.

At line:1 char:1

+ get-process -Name ping

+ ~~~~~~~~~~~~~~~~~~~~~

+ CategoryInfo : ObjectNotFound: (ping:String) [Get-Process], ProcessCommandException

+ FullyQualifiedErrorId : NoProcessFoundForGivenName,Microsoft.PowerShell.Commands.GetProcessCommand

Błąd PowerShell! Na hoście kontenera nie istnieje proces PING. Oznacza to, że z powodu izolacji Hyper-V, a zwłaszcza izolacji trybu jądra, zasoby jądra nie są współużytkowane między hostem kontenera a kontenerami Hyper-V.

Dla tych, którzy otrzymują następujący błąd:

PS C:\Users\Administrator> docker run --rm -it --name nanohyperv --isolation=hyperv microsoft/nanoserver:latest

C:\Program Files\Docker\docker.exe: Error response from daemon: container 2f83bfc2bbbbed5a0425a0219a7a747c971a1eeb032ce11b76149f17b397f17b en

countered an error during CreateContainer: failure in a Windows system call: No hypervisor is present on this system. (0xc0351000)

Oznacza to, że rola Hyper-V nie jest zainstalowana w systemie, więc nie można uruchamiać kontenerów Hyper-V. Jeśli mamy problemy z używaniem określonego kontenera, można użyć polecenia Docker Logs, aby rozwiązać problem. Polecenie dzienników Dockera wyświetla informacje zarejestrowane przez uruchomiony kontener. Zarejestrowane informacje i format dziennika zależą niemal wyłącznie od polecenia endpoint kontenera:

PS > docker logs NanoWithHYPV

52. Chronione maszyny wirtualne w Hyper-V (Shielded VM)

Ekranowana maszyna wirtualna Microsoft Hyper-V to funkcja zabezpieczeń, wprowadzona w systemie Windows 2016. Chroni ona maszynę wirtualną Hyper-V drugiej generacji przed dostępem lub naruszeniem poprzez zastosowanie kombinacji technik, takich jak: Bezpieczne uruchamianie, szyfrowanie Bit-locker, wirtualny moduł Trusted Platform i Host Guardian Service.

Ponieważ maszyna wirtualna jest plikiem, pod względem przechowywania, w pamięci, musi być zabezpieczona przed atakami za pośrednictwem systemu pamięci masowej, sieci lub podczas tworzenia kopii zapasowej.

Zakres tego bloga jest ograniczony do minimalnej konfiguracji umożliwiającej skonfigurowanie roli Host Guardian Service i odpowiednich składników wsparcia Hyper-V do zapewnienia osłoniętej maszyny wirtualnej na chronionym hoście.

52.1. Komponenty wymagane do skonfigurowania chronionego środowiska VM

W tym dziale opisano minimalną konfigurację do skonstruowania chronionego środowiska Hyper-V.

W tym przypadku chronione środowisko składa się z jednej maszyny fizycznej / wirtualnej Windows 2012/2016 w celu zapewnienia wyprodukowanego kontrolera domeny, jednej maszyny fizycznej / wirtualnej Windows 2016 DataCenter do świadczenia usługi Host Guardian (HGS), jednej maszyny fizycznej Windows DataCenter do zapewniania chronionych hostów oraz jednej lub więcej ekranowanych maszyn wirtualnych (generacja 2 maszyn wirtualnych) obsługiwanych na chronionych hostach.

Oto szczegóły maszyny z ich adresami IP:

AD Server 192.168.102.100

Host Guardian Service Node 192.168.102.101

Guarded Host Node 192.168.102.102

VM 192.168.102.103

Przed wdrożeniem ekranowanych maszyn wirtualnych w produkcji należy się upewnić, że zainstalowano najnowszą aktualizację zbiorczą zarówno w węźle usługi Host Guardian, jak i w chronionym węźle hosta.

52.2. Konfiguracja węzła HGS

Aby skonfigurować węzeł HGS, np. na serwerze Windows 2016 centrum danych należy włączyć rolę usługi Host Guardian. Tutaj odbywa się to za pomocą narzędzia Powershell.

1. Należy włączyć rolę Host Guardian Service, otwierając okno powershell w trybie podniesionym i uruchomić następujące polecenie.

Install-WindowsFeature -Name HostGuardianServiceRole -IncludeManagementTools -Restart

2. Teraz należy zainstalować domenę HGS w swoim własnym lesie, uruchamiając poniższe polecenie.

$adminPassword = ConvertTo-SecureString -AsPlainText '<password>' -Force

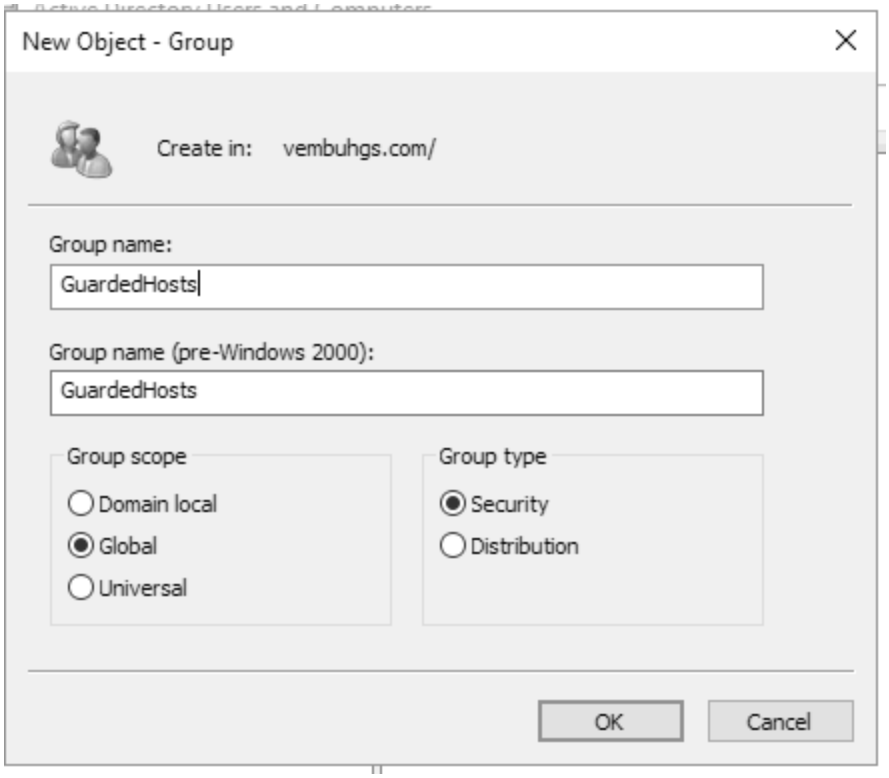
Uwaga: Należy zastępić <Password> z hasłem maszyny HGS.

Install-HgsServer -HgsDomainName 'Vembutechhgs.net' -SafeModeAdministratorPassword $adminPassword -Restart

Uwaga : Należy zastąpić ‘Vembutechhgs.net’ z fqdn naszego wyboru.

3. Po ponownym uruchomieniu komputera należy się zalogować na konto domeny przy użyciu tego samego hasła, które zostało użyte dla konta lokalnego.

52.3. Inicjalizacja węzła HGS



Aby zainicjować węzeł HGS, administrator musi mieć poprawny certyfikat SSL. W środowisku laboratoryjnym można użyć certyfikatu z podpisem własnym. Ale do użytku produkcyjnego, trzeba kupić certyfikat SSL od dostawców certyfikatów cyfrowych.

$CertificatePassword = ConvertTo-SecureString -AsPlainText '<password>' -Force

Uwaga: Należy zmienić <Password> z hasłem maszyny HGS.

$signingCert = New-SelfSignedCertificate -DnsName "signing.Vembutechhgs.net"

Export-PfxCertificate -Cert $signingCert -Password $CertificatePassword -FilePath 'C:\signingCert.pfx'

$encryptionCert =New-SelfSignedCertificate -DnsName "signing.Vembutechhgs.net"

Export-PfxCertificate -Cert $encryptionCert -Password $certificatePassword -FilePath 'C:\encryptionCert.pfx'

Następnie należy zainicjować węzeł HGS.

Initialize-HgsServer -HgsServiceName 'Hgs' -SigningCertificatePath 'C:\signingCert.pfx' -SigningCertificatePassword $certificatePassword -EncryptionCertificatePath 'C:\encryptionCert.pfx' -EncryptionCertificatePassword $certificatePassword -TrustTpm

Aby warunkowe przekazywanie wskazało sfabrykowaną domenę, należy wykonać poniższe polecenie.

Add-DnsServerConditionalForwardZone -Name "vembutech.net" -ReplicationScope "Forest" -MasterServers 192.168.102.100

Tutaj sfabrykowana domena fqdn to vembutech.net z IP 192.168.102.100.

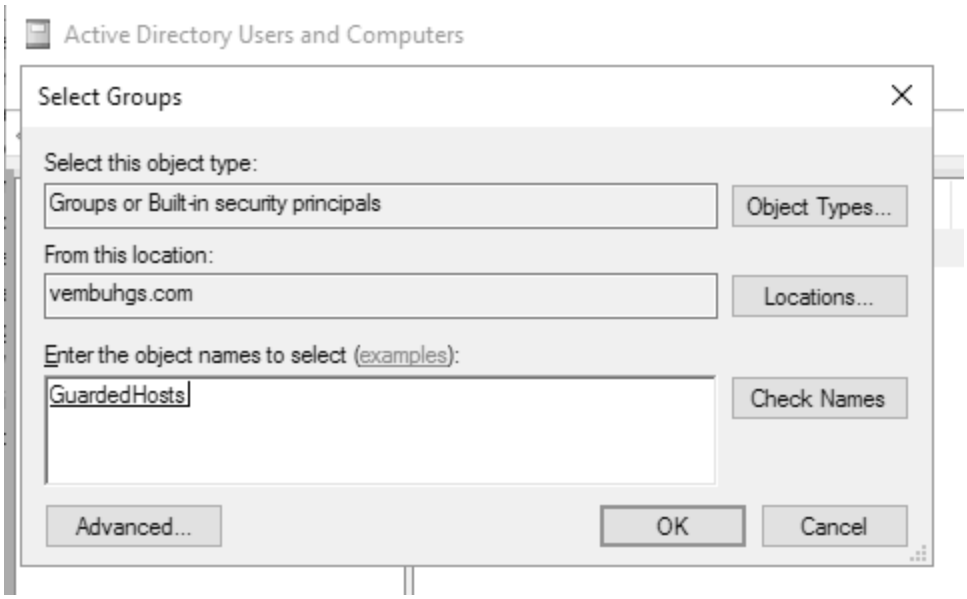
Aby dodać vembutech.net do zaufanej grupy, należy uruchomić poniższe polecenie.

netdom trust vembutechhgs.net /domain:vembutech.net /userD:vembutech.net\Administrator /passwordD: <PASSWORD> /add

Uwaga: Należy zmienić <PASSWORD> z odpowiednimi danymi uwierzytelniającymi.

To wszystko, zakończono konfigurację serwera HGS, teraz można się połączyć z kontrolerem domeny wytwórcy i wykonać poniższe czynności.

52.4. Konfiguracja kontrolera domeny wykonawcy



1. należy dodać strzeżonego hosta do domeny AD.

2. Należy utworzyć grupę o nazwie „GuardedHosts” z zakresem jako „Globalny” i typem grupy jako „Zabezpieczenie”, tak jak jest ona dołączona do obrazu w kroku 3.

Teraz należy dodać dostępny strzeżony serwer hosta do nowo utworzonej grupy, przechodząc do Komputer, należy kliknąć prawym przyciskiem Strzeżonego hosta i wybrać Dodaj do grupy.

Uwaga: Jest to przy założeniu, że strzeżony host: 192.168.102.103 jest już częścią sfabrykowanego kontrolera domeny, jeśli nie, należy to zrobić najpierw, przed przystąpieniem do tego kroku.

4. Należy wpisać nazwę grupy jako „GuardedHosts” w polu obiektu i nacisnąć przycisk Sprawdź nazwę.

5. Teraz należy dodać warunkowe przekierowanie do nazwy domeny HGS, aby to zrobić, trzeba otworzyć usługę DNS na swoim hoście AD.

6. Należy kliknąć prawym przyciskiem myszy Warunkowe forwardery i wybrać New Waritional Forwarders.

7. Należy wpisać swoją nazwę domeny HGS „Vembutechhgs.net” i podać jej adres IP – 192.168.102.101, aby dodać.

8. Teraz należy otworzyć PowerShell w trybie podwyższonym na serwerze AD i wywołać poniższe polecenie.

Get-ADGroup "GuardedHosts" | Select-Object SID

9. Należy zapisać wynikowy identyfikator SID i odłożyć go na bok. Np.: S-1-5-21-1715446949-429339150-1483827033-1107.

10. Teraz można się już z powrotem przełączyć do Power Shella serwera HGS, jako administrator, i wywołać poniższe polecenie.

Add-HgsAttestationHostGroup -Name "GuardedHosts" -Identifier "S-1-5-21-1715446949-429339150-1483827033-1107"

Uwaga: Należy zastąpić SID rezultatem z kroku 9.

10. To verify added HgsAttestation, invoke below command.

Get-HgsAttestationHostGroup

Po sukcesie można zobaczyć wynik jak poniżej.

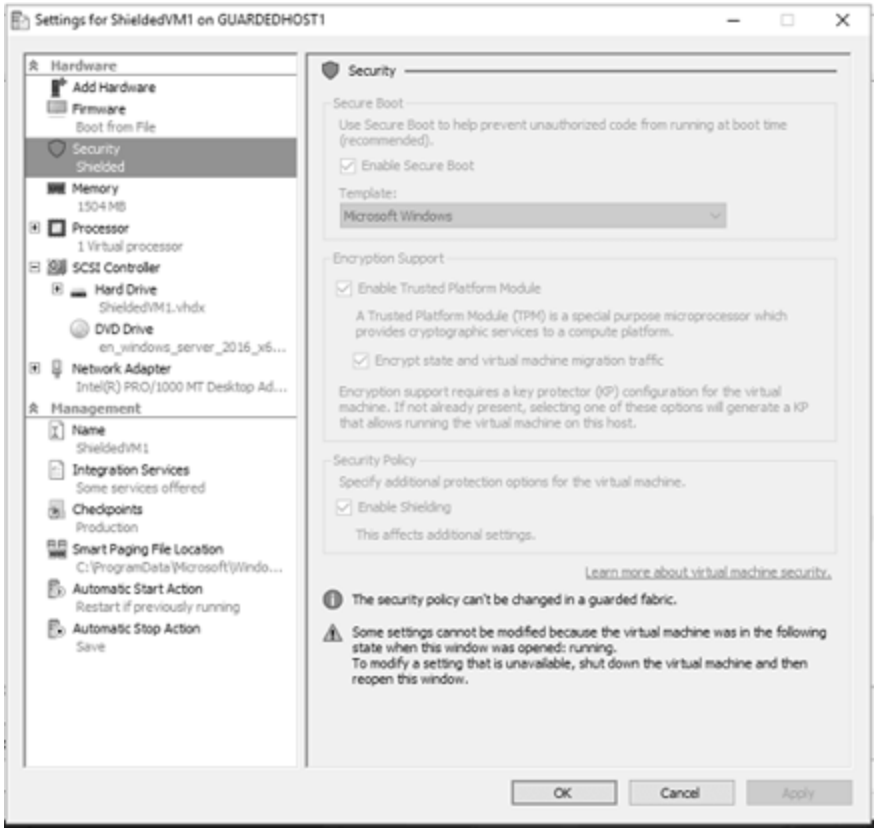
Name Identifier

---- ----------

GuardedHosts S-1-5-21-1715446949-429339150-1483827033-1107

W tym momencie skończymy z wszystkimi ustawieniami konfiguracji na hostach AD i HGS, teraz należy przejść do strzeżonej konfiguracji hosta.

52.5. Konfiguracja hosta strzeżonego



Na strzeżonym hoście należy utworzyć politykę integralności kodu, wykonując sekwencyjnie poniższe polecenia.

1. New-CIPolicy -Level FilePublisher -Fallback Hash -FilePath 'C:\HWLCodeIntegrityc.xml'

ConvertFrom-CIPolicy -XmlFilePath 'C:\HWLCodeIntegrityc.xml' -BinaryFilePath 'C:\HWLCodeIntegrityc.p7b'

2. Należy skopiować plik „C:\HWLCodeIntegrityc.p7b” do HGS server[192.168.102.101] to the root drive location [i.e] C:/.

3. Następnie należy uruchomić poniższą komendę na serwerze HGS.

Add-HgsAttestationCIPolicy -Path 'C:\HWLCodeIntegrityc.p7b' -

Name 'StdGuardHost'

4. Aby uzyskać AttestationUrl i KeyProtectionUrl, należy uruchomić poniższą komendę na serwerze HGS.

Get-HgsServer

5. Po pomyślnym uruchomieniu wynik będzie wyglądał mniej więcej jak ten poniżej.

Name Value

---- -----

AttestationOperationMode AD

AttestationUrl {http://hgs.vembutechhgs.net/Attestation}

KeyProtectionUrl {http://hgs.vembutechhgs.net/KeyProtection}

6. Należy przełączyć się z powrotem na chroniony host i skonfigurować go, aby używał HGS, wywołując poniższe polecenie.

Set-HgsClientConfiguration -KeyProtectionServerUrl "http://hgs.vembutechhgs.net/KeyProtection" -AttestationServerUrl "http://hgs.vembutechhgs.net/Attestation"

Po pomyślnej weryfikacji można zobaczyć poniższy komunikat.

IsHostGuarded : True

Mode : HostGuardianService

KeyProtectionServerUrl : http://hgs.vembutechhgs.net/KeyProtection

AttestationServerUrl : http://hgs.vembutechhgs.net/Attestation

AttestationOperationMode : ActiveDirectory

AttestationStatus : Passed

AttestationSubstatus : NoInformation

7. Można także sprawdzić stan chroniony hosta na żądanie, wywołując poniższe polecenie na strzeżonym hoście.

Get-HgsClientConfiguration

8. Po wyświetleniu pomyślnego komunikatu jako IsHostGuarded true, należy wywołać poniższe polecenie, aby przejść dalej na strzeżonym hoście. Dotyczy to poniższych podetapów.

8.1. Invoke-WebRequest 'http://hgs.vembutechhgs.net/KeyProtection/service/metadata/2014-07/metadata.xml' -OutFile 'C:/VembuTechGuardian.xml'

8.2. Import-HgsGuardian -path 'C:\VembuTechGuardian.xml' -Name 'VembuTech' -AllowUntrustedRoot

8.3. $Guardian = Get-HgsGuardian -Name 'VembuTech'

8.4. $Owner = New-HgsGuardian -Name 'Owner' -GenerateCertificates

8.5. $KP = New-HgsKeyProtector -Owner $Owner -Guardian $Guardian -AllowUntrustedRoot

Uwaga: Przed dalszym postępowaniem przyjęliśmy założenie, że strzeżony host ma już vm z nazwą „ShieldedVM1”.

Należy również pamiętać przed włączeniem chronionego vm, aby upewnić się, że włączono usługę zdalnego pulpitu na vm, ponieważ nie można połączyć się z chronioną vm przy użyciu połączenia maszyny wirtualnej.

8.6. $VMName = 'ShieldedVM1'

8.7. Stop-VM -Name $VMName -Force

8.8. Set-VMKeyProtector -VMName $VMName -keyprotector

$KP.RawData

8.9. Set-VMSecurityPolicy -VMName $VMName -Shielded $true

8.10. Enable-VMTPM -VMName $VMName

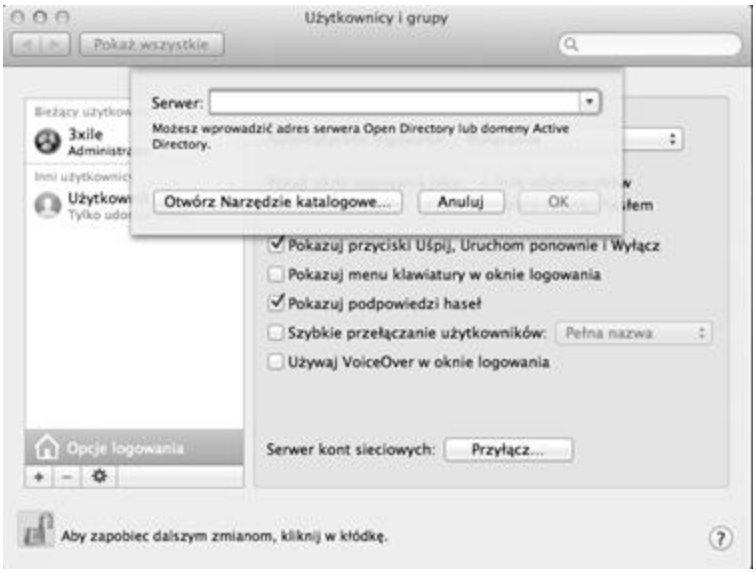
8.11. Start-VM -Name $VMName

Po pomyślnym zakończeniu powyższych kroków maszyna VM: „ShieldedVM1” stała się chroniona, można to sprawdzić, sprawdzając właściwości bezpieczeństwa VM.

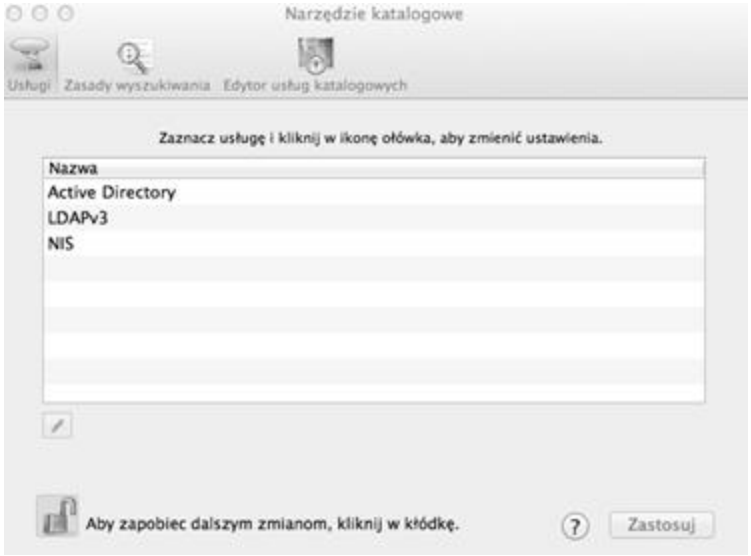
53. W jednej z sieci z Mac OS X

Komputery z systemem Mac OS X nie wymagają serwera Open Directory do pracy w domenie. Mogą one zostać połączone z dowolną usługą kompatybilną, taką jak

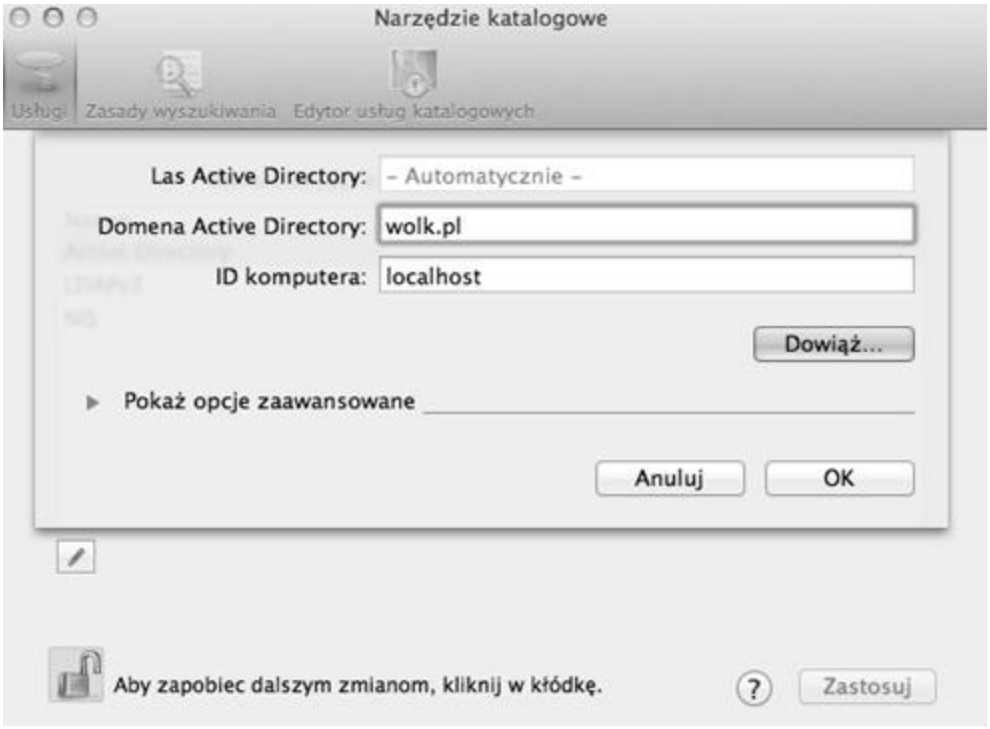
nDirectory czy Active Directory. Aby podłączyć komputer do domeny, należy uruchomić preferencje systemowe, wybrać Użytkownicy i Grupy, kliknąć w Opcje Logowania. Następnie należy kliknąć w przycisk Przyłącz obok napisu Serwer kont sieciowych. W okienku, które się pojawi, należy wybrać opcję Otwórz Narzędzie katalogowe.



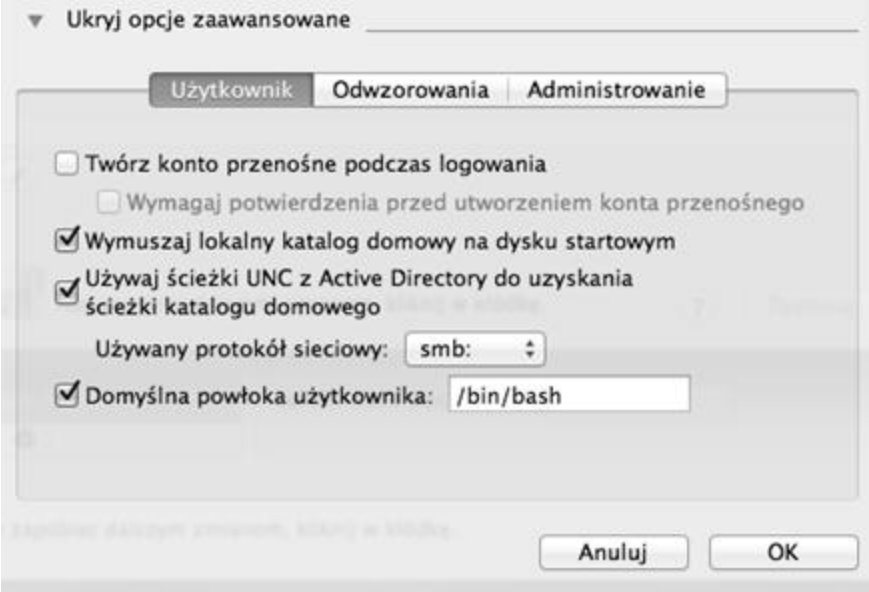
W oknie, które się otworzy należy odblokować kłódkę, klikając w nią i podając hasło administratora lokalnego. Następnie należy kliknąć dwa razy w napis Active Directory.



W polu Domena Active Directory należy wpisać domenę i kliknąć przycisk Dowiąż.

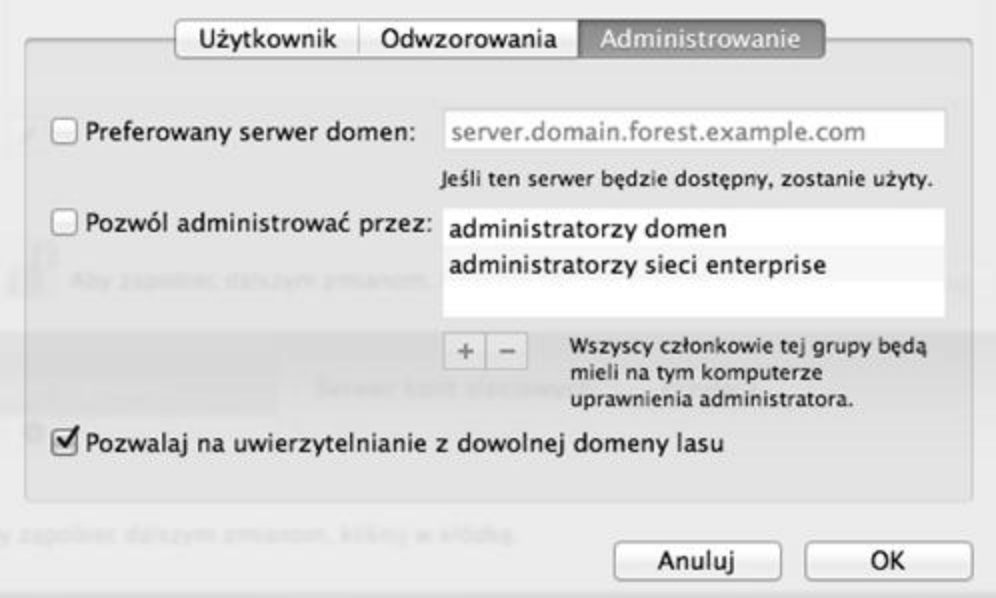


W zasadzie jest to wystarczające, jednak istnieje możliwość wprowadzenia bardziej zaawansowanych ustawień. Wystarczy kliknąć Pokaż opcje zaawansowane, aby okienko się wydłużyło i wyświetliło dodatkowe ustawienia. W zakładce Użytkownik jest możliwość utworzenia przenośnego konta podczas logowania wraz z wymuszeniem potwierdzenia jego założenia. Można także wymusić założenie lokalnego katalogu domowego na dysku startowym, czy użycia ścieżki UNC z Active Directory do uzyskania ścieżki do katalogu domowego. Do tego katalogu można się dostać przy użyciu protokołu SMB lub AFP. Można także określić miejsce, gdzie znajduje się domyślna powłoka użytkownika.

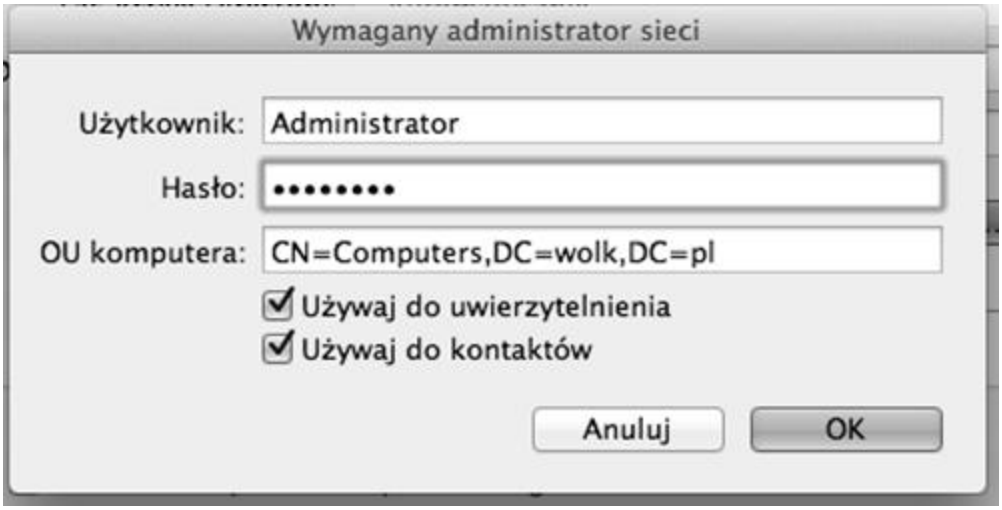


W zakładce Odwzorowania można z Active Directory pobrać i odwzorować atrybut UID, GID użytkownika oraz GID.

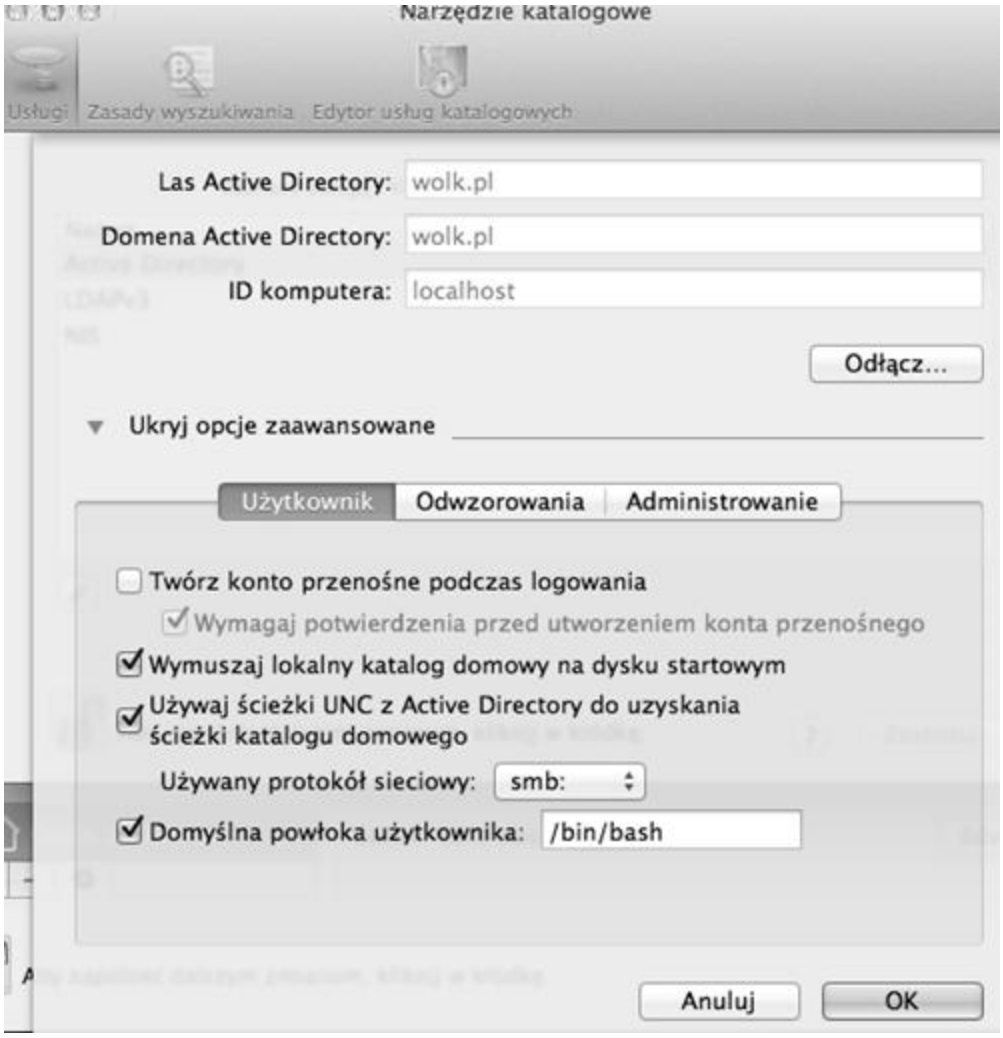
Zakładka Administrowanie pozwala określić preferowany serwer domen, jak również zdefiniować użytkowników domeny, którzy będą mogli administrować tym komputerem. Można także pozwolić na uwierzytelnianie z dowolnej domeny w lesie.



Nie mniej jednak, po kliknięciu przycisku Dowiąż pojawi się okienko, w którym trzeba podać dane użytkownika należącego już do domeny, mającego już uprawnienia do dołączania komputerów do domeny.

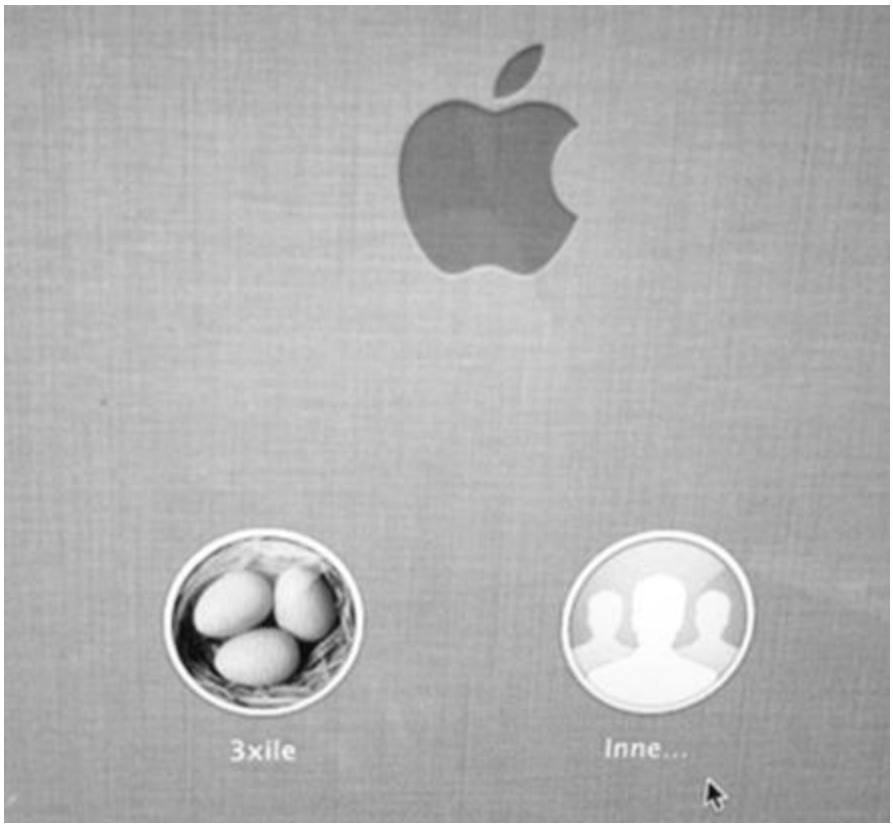


Proces dołączania może potrwać kilka minut. Gdy się zakończy, przycisk Dowiąż zostanie zamieniony na Odłącz, wystarczy kliknąć przycisk OK, aby zakończyć.



W preferencjach systemowych użytkownicy i grupy, obok napisu serwer kont sieciowych powinna pojawić się domena wraz z towarzyszącą zieloną ikoną symbolizującą łączność z kontrolerem domeny.

Od tej pory na ekranie logowania pojawi się ikona Inne, którą należy wybrać w celu zalogowania się jako użytkownik domeny.



Po jej wybraniu należy podać nazwę użytkownika oraz hasło podane w usłudze katalogowej.

Pierwsze logowanie użytkownika, jako że tworzone są jego profile i wprowadzane są ustawienia, trwa najdłużej, dlatego należy uzbroić się w cierpliwość. Od tej pory

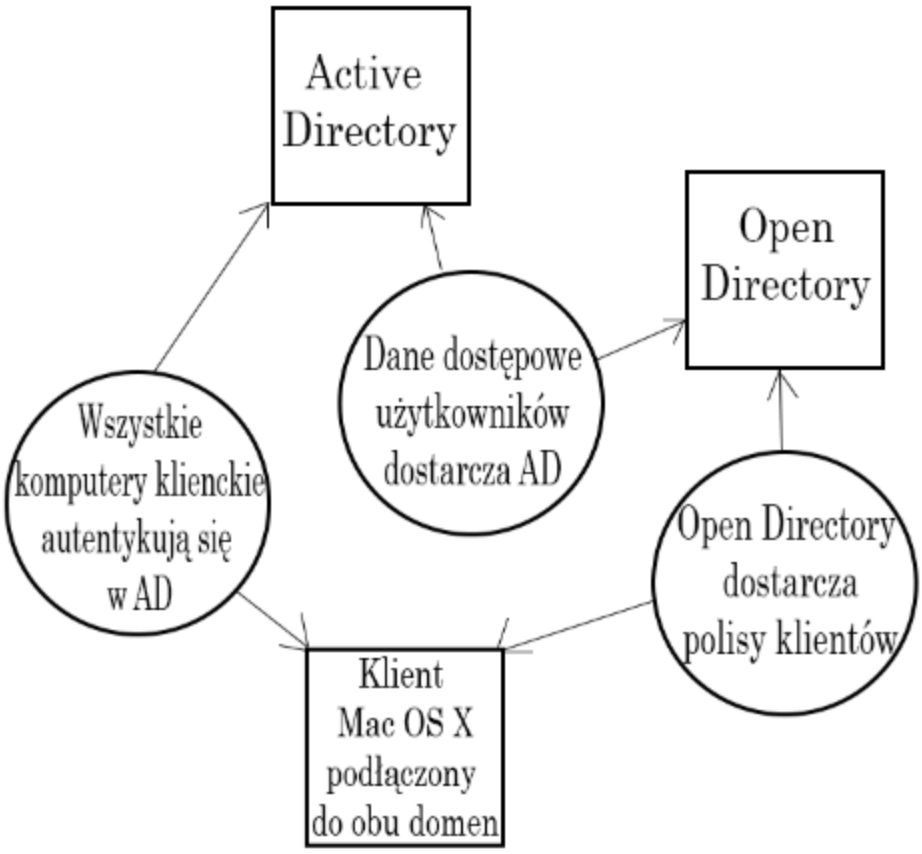
komputer jest podłączony do domeny Active Directory i może w niej współpracować z innymi maszynami.

Jeżeli występują jakiekolwiek problemy z łącznością w domenie, można próbować dochodzić problemu ręcznie lub posłużyć się komendą konsolową, która wyświetli informacje na temat aktualnej konfiguracji. Te informacje pozwolą w sposób łatwiejszy wywnioskować, gdzie leżą ewentualne problemy. Wystarczy w terminalu podać polecenie dsconfigad –show. To, czy komputer ma łączność z domeną, można sprawdzić także komendami dscl /Active\ Directory/All\ Domains – list /Users lub id –p nazwa_użytkownika. Jeżeli któreś z poleceń zwróci odpowiedź, znaczy, że jest łączność z kontrolerem domeny.

Aby podpiąć komputer do domeny Active Directory za pomocą konsoli, należy wydać polecenie dsconfigad –a konto_komputera \ -domain wolk.pl \ -u Administrator –p hasło_administratora_domeny \ -lu administrator_lokalny –lp hasło_administratora_lokalnego.

Faktem, którego nie da się ukryć, jest to, że w większości środowisk firmowych dominują rozwiązania firmy Microsoft. Choć komputery pod kontrolą Mac OS X można bezproblemowo podpiąć do domeny Active Directory, to nie ma innego sposobu zarządzania takim komputerem, czy jego uprawnieniami, bez obecności Mac OS X Server. Tak zwany Magiczny Trójkąt polega właśnie na tym, aby za autentykację odpowiadał serwer Active Directory, natomiast za narzucanie polis bezpieczeństwa serwer Open Directory.

Serwery między sobą powinny być tak skonfigurowane, aby mogły wymieniać dane, a stacje klienckie powinny być podłączone do dwóch domen jednocześnie. Wszystkie komputery powinny korzystać z tych samych serwerów DNS, a serwery DNS powinny przechowywać zarówno strefę wyszukiwania do przodu, jak i strefę wyszukiwania wstecz.



Zanim administrator przystąpi do konfiguracji, powinien zapoznać się z tematyką Windows Server z zakresu Active Directory oraz DNS. Stosowne działy znajdują się w niniejszej publikacji. Jeżeli zagadnienia te są użytkownikowi znane, można je pominąć.

53.1. Konfiguracja Magic Triangle

Bardzo ważnym etapem konfiguracji są ustawienia serwera DNS. Po stronie serwera Windows Server zainstalowano usługę Active Directory i stworzono jednego użytkownika o nazwie testowy.

Wraz z Active Directory został zainstalowany serwer DNS, w którym znalazły się dwa wpisy Host A: wolk-dc01, wskazujący na kontroler domeny Active Directory, oraz wolk-mac, wskazujący na kontroler domeny Open Directory. Naturalnie nazwy komputerów muszą odzwierciedlać wpisy w serwerze DNS.

Konfiguracja sieci w przykładzie jest następująca:

Kontroler AD:

- domena wolk.pl,
- adres IP: 192.168.0.1,
- maska: 255.255.255.0.

Kontroler OD:

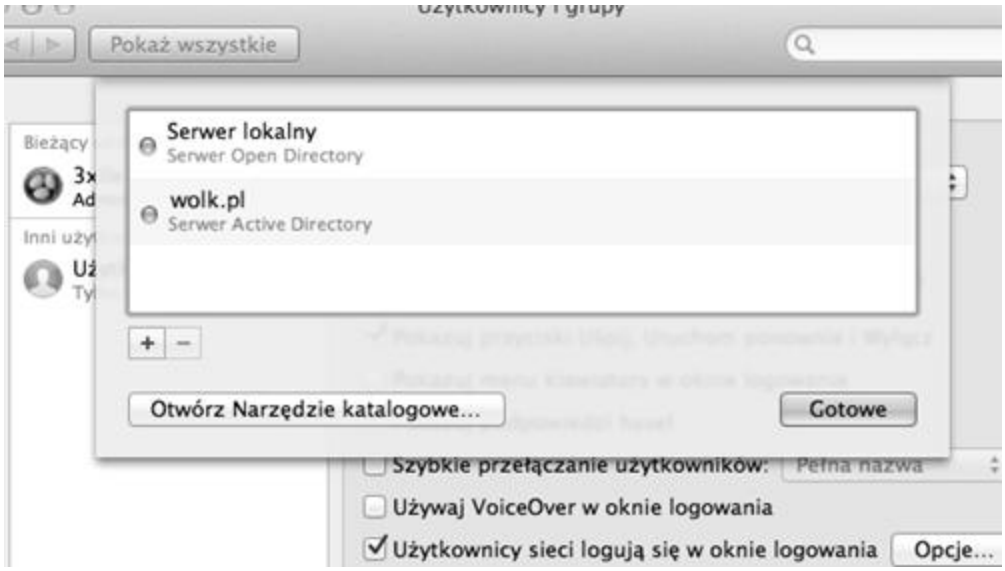
- domena mac.wolk.pl,
- adres IP: 192.168.0.2,
- maska: 255.255.255.0,
- router: 192.168.0.1,
- DNS główny: 192.168.0.1,
- DNS zapasowy: 127.0.0.1.

Stacja robocza:

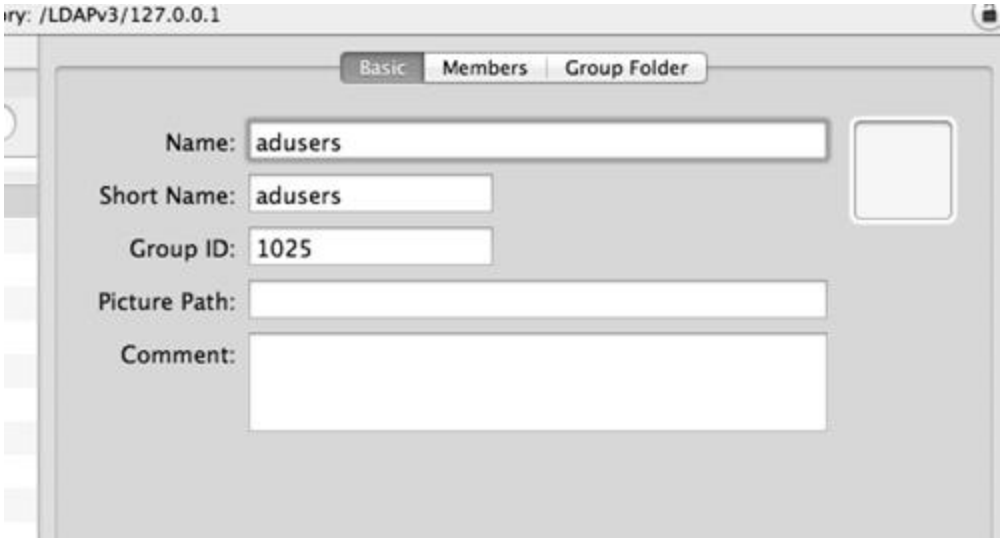
- adres IP: 192.168.0.3,
- maska: 255.255.255.0,
- router: 192.168.0.1,
- DNS główny: 192.168.0.1,
- DNS zapasowy: 192.168.0.2.

W pierwszej kolejności należy uruchomić usługę Open Directory, tworząc domenę mac.wolk.pl oraz nadając komputerowi nazwę wolk-mac. Należy pamiętać, aby wcześniej wprowadzić odpowiednią konfigurację sieci.

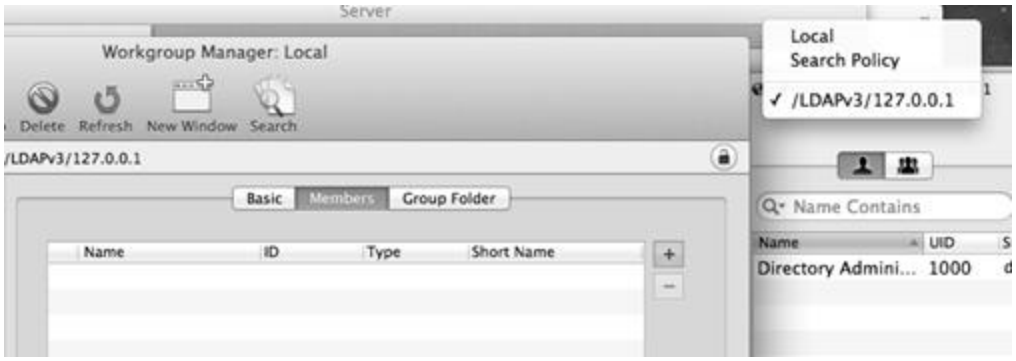
Następnie należy serwer podłączyć do domeny Active Directory. Robi się to w sposób analogiczny do podłączania zwykłej stacji roboczej. Nie ma potrzeby zmiany żadnych ustawień zaawansowanych. Po tym procesie komputer powinien być w dwóch domenach: jednej, lokalnej, którą sam hostuje oraz zewnętrznej Active Directory.



Następnie należy uruchomić Workgroup Menager na serwerze OD. Teraz należy zautentykować się jako diradmin dla zasobów Open Directory. Dalej trzeba stworzyć grupę adusers (nazwa jest dowolna), w której będą przechowywane obiekty z Active Directory.



Następnie należy dodać do tej grupy obiekty, które powinny pochodzić z Active Directory. Należy kliknąć Members, następnie w plusik „+", a dalej w granatowe kółeczko przy napisie Directory i wybrać pożądaną domenę Active Directory.



W liście po prawej stronie zostaną wyświetleni użytkownicy Active Directory. Tych, którymi administrator pragnie zarządzać, należy przeciągnąć do grupy.

Dla testu wprowadzono preferencje użytkownika w sekcji Applications i Finder. Powinna uruchamiać się tylko przeglądarka Safari, a Finder powinien zostać uproszczony.

Ostatnim krokiem będzie przyłączenie stacji roboczej do obu domen. W teście w laboratorium przyłączono stację roboczą najpierw do domeny Active Directory, a następnie do Open Directory. Dla przeprowadzenia testu można zalogować się na użytkowniku testowy i zweryfikować to, że preferencje zostały zaaplikowane.

Ostatnią rzeczą, jaką należy uruchomić, jest Single Sign-On. Mechanizm ten należy najpierw uruchomić w Active

Directory. Po stronie Mac OS X należy wejść do folderu /Applications/Utilities i wydać tam polecenie:

sudo dsconfigad –enablesso

Gdyby magiczny trójkąt nie działał poprawnie, problemem najprawdopodobniej będzie błędna konfiguracja serwera DNS, brak synchronizacji serwera czasu lub problemy z replikacją danych pomiędzy serwerami.

Dziękujemy za skorzystanie z oferty naszego wydawnictwa i życzymy miło spędzonych chwil przy kolejnych naszych publikacjach.

Wydawnictwo Psychoskok